(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2003 (02.10.2003)

PCT

(10) International Publication Number
WO 03/081519 A2

(51) International Patent Classification[7]: G06K 7/00

(21) International Application Number: PCT/US03/08638

(22) International Filing Date: 19 March 2003 (19.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/366,098 19 March 2002 (19.03.2002) US
60/379,964 13 May 2002 (13.05.2002) US

(71) Applicant: CHAMELEON NETWORK INC. [US/US]; Suite 1400, 950 Winter Street, Waltham, MA 02451 (US).

(72) Inventors: THOMAS, Joseph, A.; 34 Warren Street, Westborough, MA 01581 (US). JESSEN, Karlin, B.; 97 Pleasant Street, Reading, MA 01867 (US). BURGER, Todd, O.; 386 Lincoln Street, Lexington, MA 02421 (US). HASSOL, Joshua, L.; 28 Wachusett Drive, Lexington, MA 02421 (US).

(74) Agent: PRITZKER, Randy, J.; Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210 (US).

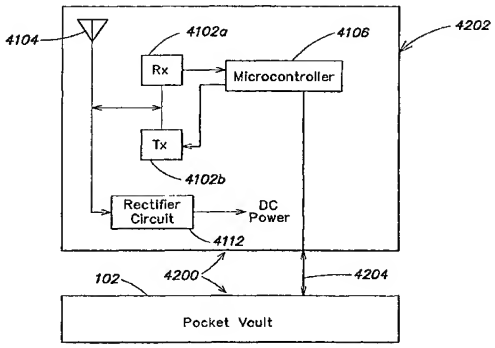
(81) Designated State *(national)*: CA.

(84) Designated States *(regional)*: European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD



(57) Abstract: In one embodiment, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user. In another embodiment, an apparatus comprises, a memory, a user input, and a transponder. The memory stores at least first and second distinct codes. The user input permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal. The transponder emits a wireless signal representing the selected one of the at least first and second code sin response to an interrogation signal. In yet another embodiment, a token that may be used to engage in a transaction at a point of sale comprises a substrate, a rewritable memory, and a reconfigurable display. The rewriteable memory is supported by the substrate and can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale. The substrate and memory are configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The reconfigurable display is also supported by the substrate and displays at least some of the information that is stored in the rewritable memory.

WO 03/081519 A2

PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD

RELATED APPLICATIONS

This application is a Continuation-in-Part (CIP) of Application Serial No. 09/968,628, filed October 1, 2001, and now pending, which is a CIP of U.S. Application Serial No. 09/675,438, filed September 28, 2000, and now pending, which claims the benefit of each of: (1) Application Serial No. 60/156,356, filed September 28, 1999; (2) Application Serial No. 60/167,050, filed November 23, 1999; (3) Application Serial No. 60/184,425, filed February 23, 2000; and (4) Application Serial No. 60/217,542, filed July 12, 2000. This application also claims the benefit of each of (1) Application Serial No. 60/366,098, filed March 19, 2002, and (2) Application Serial No. 60/379,964, filed May 13, 2002.

FIELD OF THE INVENTION

The present inventions are directed to novel systems and methods for engaging in transactions involving financial and/or non-financial media.

BACKGROUND OF THE INVENTION

People often times carry wallets with them when they engage in their day to day activities. A typical wallet is made of leather or other suitable material, and is generally a foldable structure that readily fits into a pocket or purse. A wallet typically includes a number of pockets, pouches, or the like for storing items such as a driver's license, a social security card, identification cards, credit cards, debit cards, membership cards, commuter passes, access tools, business cards, cash, coupons, event tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipts, photographs, etc.

Wallets are frequently stolen, lost, or misplaced. When any of these events occurs, not only must the wallet itself be replaced, but all of the contents of the wallet must be replaced as well. As anyone who has lost a wallet can testify, replacing the contents of a wallet can be cumbersome and expensive. In addition, if a wallet is stolen or if a lost wallet falls into the wrong hands, the contents of the wallet may be used to engage in unauthorized activities which financially detriment the wallet owner, as well as

any banks, credit issuers, and/or other institutions that issued financial media to the wallet owner.

While the wallet owner is generally able to "cancel" financial media in such situations by contacting the respective financial media issuers, often times this is done too late, i.e., after one or more media have been exploited by the unauthorized user. In some cases, the wallet owner may not recall all of the contents of the now stolen wallet, and so may fail to report theft of one or more items. Further, in addition to any cash contained in a lost or stolen wallet, many media issued by non-financial media issuers have a significant cash value, e.g., transportation tickets, event tickets, commuter passes, and the like, and therefore represent an immediate (and often times unrecoverable) financial loss to the wallet owner. Moreover, the misappropriation of media issued by non-financial media issuers that contain personal information, e.g., a drivers license, social security card, identification card, etc., present the opportunity for an unauthorized possessor of a wallet to engage in the practice known as "identity theft," whereby the possessor may assume the identity of the wallet owner for various fraudulent purposes, e.g., using the assumed identity to obtain and exploit one or more new financial media.

Another device commonly used to engage in or authorize transactions is a radio frequency identification (RFID) tag. In an RFID system, an "interrogator" broadcasts a radio frequency (RF) signal which, if received by an RFID tag, causes the RFID tag to return an RF signal to the interrogator that includes information from the tag that may be used to authorize a transaction. Situations in which such tags have been employed include, e.g., automated toll booths and gasoline service stations. RFID tags may be made relatively small in size and therefore may be kept virtually anywhere, e.g., on a keychain or clipped to an automobile visor. Unfortunately, while this aspect of these devices make them convenient, it also makes them highly susceptible to loss or theft. Whenever an RFID tag falls into the wrong hands, there is potential for it to be misused for a long period of time before it is discovered to be missing and some action is take to disable the account associated with it so that it can no longer be used to authorize transactions.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal

representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user.

According to another aspect, an apparatus comprises, a memory, a user input, and a transponder. The memory stores at least first and second distinct codes. The user input permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal. The transponder emits a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

According to yet another aspect, a token that may be used to engage in a transaction at a point of sale comprises a substrate, a rewritable memory, and a reconfigurable display. The rewriteable memory is supported by the substrate and can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale. The substrate and memory are configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The reconfigurable display is also supported by the substrate and displays at least some of the information that is stored in the rewritable memory.

According to another aspect, a method for using an apparatus comprises steps of using the apparatus to authenticate an identity of a user of the apparatus, and after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal.

According to another aspect, a method for using an apparatus comprises steps of manipulating a user input on the apparatus to select one of at least first and second codes stored in memory, and permitting a transponder of the apparatus to emit a wireless signal representing the selected one of the at least first and second codes in response to a wireless interrogation signal.

According to yet another aspect, a method for configuring a token to be used to engage in a transaction at a point of sale involves a step of configuring a rewritable memory of the token to store information that identifies an account that may be used to engage in the transaction at the point of sale. The memory is configured and arranged on the token such that the token can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The method further

involves a step of configuring a display on the token to display at least some of the information that is stored in the rewritable memory.

According to another aspect, a method is disclosed for enabling a software module on a computer operated by a user to access restricted information on a server. With an electronic device distinct from the computer, an identity of the user is authenticated to determine that the user is permitted to access the restricted information on the server. In response to the electronic device authenticating the identity of the user, the software module on the computer is permitted to access the restricted information on the server.

According to another aspect, a method is disclosed for altering settings on a computer to correspond to settings on an electronic device distinct from the computer. With the electronic device, an identity of a user is authenticated to determine that the user is authorized to use the electronic device. In response to authenticating the identity of the user, the settings on the computer are altered to correspond to settings on the electronic device.

According to another aspect, a system for enabling a software module on a computer operated by a user to access restricted information on a server includes an electronic device which includes a user-authenticator to authenticate an identity of the user to determine that the user is permitted to access the restricted information on the server. The system further comprises means for, in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

According to yet another aspect, a system for altering settings on a computer to correspond to settings on an electronic device distinct from the computer comprises a user authenticator included in the electronic device to authenticate an identity of a user to determine that the user is authorized to use the electronic device. The system further comprises means for, in response to authenticating the identity of the user, altering the settings on the computer to correspond to settings on the electronic device.

According to another aspect, an apparatus includes a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory, supported by the housing, that stores transaction information for at least first and second media; and at least one output, supported by the housing, that releases at

least a portion of the transaction information to a point-of-sale (POS) terminal after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: (a) storing transaction information for at least first and second media in a memory of a device (b) using the device to authenticate an identity of a user; and (c) after authenticating the identity of the user with the device, transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus.

According to another aspect, a method involves steps of: storing transaction information for at least one media in a memory of a first device; using the first device to authenticate an identity of a user; and after authenticating the identity of the user with the first device, releasing an embedded identification code of the apparatus from the housing that enables a second device receiving the embedded identification code to authenticate the identity of the first device.

According to another aspect, an apparatus includes: at least one memory that stores transaction information for at least first and second media; at least one input that enables a user to select one of the at least first and second media; a display that provides a visual indication to the user regarding which of the at least first and second media has been selected with the at least one input; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect, a method involves steps of: storing transaction information for at least first and second media in a memory of a device; receiving as input a user's selection of one of the at least first and second media; displaying a visual indication to the user regarding which of the at least first and second media has been selected; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, an apparatus includes: at least one memory that stores transaction information for at least one financial media and at least one non-financial media; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect, a method involves steps of: storing transaction information for at least one financial media and at least one non-financial media in a memory of a device; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, a system includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a device releasably attached to the housing; and configuring means, supported by the housing, for selectively configuring the device to hold the transaction information so that the device may be used to engage in a transaction involving the at least one media.

According to another aspect, a method involves steps of: (a) storing transaction information for at least one media in a memory of a first device, the first device having a second device releasably attached thereto; (b) while the second device is attached to the first device, configuring the second device to hold the transaction information for the at least one media based on the contents of the memory; (c) detaching the second device from the first device; and (d) using the second device to engage in a transaction involving the at least one media.

According to another aspect, a system includes: a first device including a user authenticator that authenticates an identity of a user; and a second device releasably attached to the first device, wherein the second device holds transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media, and wherein the second device is detached from the first device after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: with a first device, authenticating an identity of a user; and after authenticating the identity of a user with the first device, detaching a second device from the first device, the second device holding transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media.

According to another aspect, a system includes: a first device; a second device that has the first device releasably attached thereto, the second device including means for selectively configuring the first device to hold transaction information for a first media but not for a second media so that the first device may be used to engage in a transaction involving the first media but not the second media, and the second device further including means for selectively configuring the first device to hold transaction information for the second media but not for the first media so that the first device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect, a method involves steps of: selectively configuring a device to hold transaction information for a first media but not for a second media so that the device may be used to engage in a transaction involving the first media but not the second media; and selectively configuring the device to hold transaction information for the second media but not the first media so that the device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect, a system includes: at least one memory that stores first transaction information for a first media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively add second transaction information for a second media to the memory.

According to another aspect, a method involves steps of: storing first transaction information for a first media in a memory of a device; releasing at least a portion of the first transaction information to a point-of-sale (POS) terminal; and in response to a request by the person to whom the first transaction information is issued, adding second transaction information for a second media to the memory.

According to another aspect, a system includes: at least one memory that stores first transaction information for a first media and second transaction information for a second media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively remove at least a portion of the second transaction information from the memory.

According to another aspect, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in a memory of a device; releasing at least a portion of the first transaction information to a

point-of-sale (POS) terminal; and, in response to a request by the person to whom the second media is issued, removing at least a portion of the second transaction information from the memory.

According to another aspect, a system includes: at least one memory that stores transaction information for at least one media; at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal; and means for enabling at least one functional characteristic of the at least one media to be altered by altering the contents of the least one memory.

According to another aspect, a method involves: storing transaction information for at least one media in a memory of a device; releasing at least a portion of the transaction information to a point-of-sale (POS) terminal; and altering at least one functional characteristic of the at least one media by altering the contents of the least one memory.

According to another aspect, an apparatus includes: a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory that, supported by the housing, stores first transaction information for a first media and second transaction information for a second media; and at least one output, supported by the housing, that releases the first transaction information only after the user authenticator has authenticated the identity of the user, and that releases the second information without requiring the user authenticator to have authenticated the identity of the user.

According to another aspect, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in at least one memory of a device; using the device to authenticate an identity of a user; releasing the first transaction information only after the identity of the user has been authenticated; and releasing the second transaction information without requiring the identity of the user to be authenticated.

According to another aspect, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device causes the first device to generate a machine-readable code for only a predetermined, finite period of time after the first device is detached from the second device.

According to another aspect, a method involves a step of generating a machine-readable code on a device for only a predetermined, finite period of time.

According to another aspect, an apparatus includes: a portable substrate; a power supply supported by the substrate; and at least one controller supported by the substrate and powered by the power supply, the at least one controller being configured to generate a simulated magnetic stripe on the substrate.

According to another aspect, an method involves a step of generating a simulated magnetic stripe on a portable device.

According to another aspect, a system includes: at least one memory that stores transaction information for at least one media; a user authenticator that authenticates an identity of the user; and a display that provides a visual indication to the user regarding the at least one media, the visual indication being displayed for only a predetermined, finite period of time after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: authenticating an identity of a user; and displaying a visual indication to the user regarding the at least one media for only a predetermined, finite period of time after authenticating the identity of the user.

According to another aspect, a system includes a portable device that can be used to engage in point-of-sale (POS) transactions; and a device remote from the portable device, that can disable an ability of the portable device to engage in POS transactions.

According to another aspect, a method involves steps of: providing a portable device that can be used to engage in point-of-sale transactions; and at a location remote from the portable device, disabling an ability of the portable device to engage in POS transactions.

According to another aspect, a method involves steps of: storing transaction authorization information for at least two media in a first memory of a first device; and storing the transaction authorization information for the at least two media in a second memory, which is disposed at a location remote from the first device.

According to another aspect, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device can cause the first device to generate a machine-readable code after the first device is detached from the second device, the second device including at least one controller configured so as to be capable of causing

the first device to generate the machine-readable code only for a finite, predetermined period of time.

According to another aspect, a method involves a step of configuring a first device such that the first device is capable, for only a predetermined, finite period of time, of generating a machine-readable code on a second device.

According to another aspect, a method involves steps of: receiving information at a first device that has been transmitted over an electronic communication link; and after receiving the information at the first device, using a media at the first device to access a quantity of credit or cash reserves that could not be accessed prior to the first device receiving the information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating an example of a network system in which a portable electronic authorization device (also referred to herein as a "Pocket Vault") may be employed according to one embodiment of the invention;

Fig. 2 is a block diagram showing an illustrative embodiment of the Pocket Vault shown in Fig. 1;

Fig. 3 is a block diagram showing an illustrative embodiment of one of the interface stations shown in Fig. 1;

Fig. 4 is a block diagram showing an illustrative embodiment of the network server(s) shown in Fig. 1;

Fig. 5 is a diagram showing an example of how the memory of the Pocket Vault shown in Fig. 2 may be configured in accordance with one embodiment of the invention;

Fig. 6 is a block diagram showing an illustrative embodiment of the token (e.g., a card) associated with the Pocket Vault shown in Fig. 2;

Fig. 7 is a flow diagram illustrating a primary routine that may be executed by the controller of the Pocket Vault shown in Fig. 2;

Fig. 8 is a flow diagram illustrating an example implementation of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7;

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine shown in Fig. 10;

Fig. 12 is a flow diagram illustrating an example implementation of the VERIFY CARD RETURN routine shown in Fig. 7;

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the pocket vault interface unit shown in Fig. 3;

Fig. 14 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the interface station computer shown in Fig. 3;

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine shown in Fig. 14;

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 14;

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine in Fig. 14;

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine shown in Fig. 14;

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller(s) of the network server(s) shown in Fig. 4;

Fig. 20 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO REGISTER NEW POCKET VAULT HOLDER routine shown in Fig. 19;

Fig. 21 is a flow diagram illustrating an example implementation of the PROCESS REQUEST BY MEDIA ISSUER/ADVERTISER TO UPDATE NETWORK SERVER routine shown in Fig. 19;

Fig. 22 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 19;

Fig. 23 is a flow diagram illustrating an example implementation of the PROCESS REQUEST FROM HOLDER TO LOAD NEW FILE ONTO NETWORK SERVER routine shown in Fig. 19;

Fig. 24 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine shown in Fig. 19;

Fig. 25 is a flow diagram illustrating an example implementation of the AUTHORIZED POCKET VAULT USE? routine shown in each of Figs. 20, 22, and 24; and

Figs 26a-26p are illustrations of the portable electronic authorization device, as well as the token (e.g., a card) associated therewith, as these items may appear when in use;

Fig. 27 is a block diagram illustrating several additional features that may optionally be added to a network system such as that shown in Fig. 1 so as to enhance the functionality of the network;

Fig 28 is a block diagram illustrating example components that may optionally be added to software executing on a controller of the Pocket Vault, such as the software described in connection with Figs. 7-12, so as to enhance the functionality of the Pocket Vault in a network environment;

Fig 29 is a data flow diagram illustrating an example of how data may flow between the Pocket Vault and a user interface of an interface station computer to which the Pocket Vault is interfaced/docked;

Fig. 30 is a flow diagram illustrating an example of a primary routine that may be executed by a website on the network server(s) shown in Fig. 27, which website may be accessed, for example, by a browser executing on the interface station computer shown in Fig. 27;

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine shown in Fig. 30;

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine shown in Fig. 33;

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine shown in Fig. 33;

Fig. 36 is a flow diagram illustrating an example implementation of the RECOVERY routine shown in Fig. 33;

Fig. 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine shown in Fig. 33;

Fig. 38 is a flow diagram illustrating an example implementation of the BACKUP routine shown in Fig. 33;

Fig. 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine shown in Fig. 33;

Fig. 40 is a flow diagram illustrating an example implementation of the RFID TAG LOADING routine shown in Fig. 33;

Fig. 41 is a block diagram showing a prior art RFID tag; and

Fig. 42 is a block diagram showing an example embodiment of an RFID system in which a Pocket Vault such as that shown in Fig. 2 is used to selectively provide data to an RFID tag.

DETAILED DESCRIPTION

Disclosed herein is a new method and system for producing, distributing, storing, and using the typical contents of a person's wallet, as well as the multiple, separate transaction authorization devices, e.g., RFID tags, owned by the person. Essentially, the system may enable individuals to replace nearly all of the paper and plastic contents of their wallets and all of their other transaction authorization implements with a single, hand-held portable electronic authorization device. The system may include the portable electronic authorization devices, removable morphing tokens or cards associated with such devices, associated computer peripherals, software and certain network capabilities. As a whole, the system may eliminate virtually all of the distribution costs and security concerns associated with paper and plastic media.

Because the device may incorporate many different media that are commonly stored in a person's wallet or elsewhere, possibly including both financial and non-financial media, it is much more than a simple point-of-sale (POS) device. Therefore, the device may be more appropriately referred to as a multi-purpose, "point-of-transaction" device. In any situation of presentment, whether for purposes such as

building security, demonstrating membership or using credit or debit capacity, the system is designed to perform tasks more safely, securely and with greater ease than is possible with prior art systems. Further, while certain computer technologies are involved, the preferred embodiment is such that some people may barely recognize it as a computer, seeing instead a more comfortable to carry, easier-to-use, safer and more securely packaged means of transporting typical wallet contents and other items.

The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various financial and non-financial media, that also may enable individuals and retailers to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns.

A network system 100 configured according to one illustrative embodiment of the invention is shown in Fig. 1. As shown, the network system 100 may include a portable electronic authorization device 102 (alternatively referred to herein as a "Pocket Vault") and an associated token 102a (alternatively referred to herein as a "Chameleon Card"). Each person desiring to use the network system 100 may possess his or her own the Pocket Vault 102 and associated token 102a. Some individuals may choose to own multiple Pocket Vaults or Chameleon Cards. The system and software therefore may accommodate the use of multiple Pocket Vaults and multiple Chameleon Cards by one individual.

Referring to Fig. 1, in addition to the Pocket Vault 102, the network system 100 may include one or more network servers 114 to which various other network components are coupled. Although multiple, load-sharing network servers 114 may be employed in a typical application, the network server(s) 114 will hereinafter, for convenience, occasionally be referred to as a single network server 114. Coupled to the network server 114 are: several different types of interface stations 104 (i.e., a validation interface station 104a, a personal interface station 104b, and a commercial interface station 104c), one or more commercial card readers 106, one or more commercial bar code readers 107, one or more RFID interrogators 116, and several computers 108, 110,

and 112 operated by one or more advertisers, non-financial media issuers, and financial media issuers, respectively. The structure and functionality of each of the components of the network system 100 in accordance with illustrative embodiments of the invention are described below.

As shown in Fig. 1, the network server 114 may form the hub of the network system 100, with each of the interface stations 104, the commercial card readers 106, the commercial bar code readers 107, the RFID interrogators 116, and the computers 108, 110, and 112 being coupled thereto. As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders.

Any of a number of techniques may be used to interconnect the various elements of the network system 100, and the invention is not limited to any particular networking technique. In one illustrative embodiment, for example, the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between most of the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links).

As shown in Fig. 1, the Pocket Vault 102 may be interfaced with any of the interface stations 104a-c so as to permit information to be uploaded from the network server 114 to the Pocket Vault 102, or to be downloaded from the Pocket Vault 102 to the network server 114. In one illustrative embodiment, each of the interface stations 104 includes a docking mechanism that permits a Pocket Vault 102 to be physically, as well as electronically, interfaced therewith. In such an embodiment, once the Pocket Vault 102 is physically "docked" with an interface station 104, the Pocket Vault 102 may communicate with the interface station 104 using any now known or later discovered technique. For example, physical contact may be made between respective electrodes or plugs, a line of sight (e.g., infrared) wireless link may be established, or any other interfacing technique may be employed.

The Pocket Vault 102 may additionally or alternatively be configured such that it need not be physically docked with or even in the same room as the interface station 104, as a wireless network such as Bluetooth may be employed to permit communication between devices on the network system 100. In fact, in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114, without the interface stations 104a-c facilitating communication therebetween. In addition, in some embodiments, Pocket Vaults 102 may communicate directly with one another. In such embodiments, such inter-device communication may permit value to be exchanged directly between Pocket Vaults 102.

The personal docking station 104b may allow setting or changing of user preferences, recording of miscellaneous information by the Pocket Vault holder, replenishment or deletion of information regarding particular media, and may also permit additional media (e.g., a library card) to be added to the device. The Pocket Vault holder may, for example, directly add non-value-based media (e.g., a membership number for the local Historical Society) and notes to the Pocket Vault 102. In one embodiment, value-based and certain identification media (a driver's license, passport, building security ID, etc.) may be added or reinstated only through a secure connection to the network server 114 (as described below), in response to an update request from the Pocket Vault holder. In addition, the personal interface station may provide a mechanism to download transaction activity involving the Pocket Vault 102 into an individual's home computer. There are many users of home finance software. These applications can be relatively "data hungry," and commonly require users to download checking and debit card data from their banks (or key it in manually) and to key in the details of credit card and cash purchases. All of this keying and internet file downloading from third parties may be replaced by a simple docking procedure, i.e., when the Pocket Vault 102 is interfaced with the personal docking station 102b.

As shown in Fig. 1, and as described below in more detail, the Pocket Vault 102 may be equipped to generate the token 102a such that the token 102a has transactional information regarding a media (e.g., an actual or simulated magnetic stripe or a bar code) produced thereon. In such an embodiment, after the token 102a has been generated, the token 102a may be used by the Pocket Vault holder to engage in a transaction wherein an entity swipes the magnetic stripe portion of the token 102a through a card reader 106 or

scans the bar code on the token 102a using a bar code reader 107. Additionally or alternatively, the token 102a may include a suitable Smartcard interface so that it may be used with Smartcard compatible devices.

Because the token 102a may be caused to take on a different personality each time it is released from the Pocket Vault 102, a plurality of media may be stored electronically in memory of the Pocket Vault 102, and the token 102a may, upon request, be generated to take on the personality selected by the Pocket Vault holder. The respective media stored on the Pocket Vault 102 may be issued by different and unrelated media issuers. As used herein, two media issuers are "unrelated" if there exists no legal relationship between them.

The token 102a may also have display capacity. Such a display may, for example, indicate the media personality the token 102a has taken on. In addition, for security purposes, the account number of the media, and perhaps other information, for example, the three digit security code typically found on credit cards, may be shown on the display of the token 102a after it is ejected from the Pocket Vault. The display of this information may help prevent fraudulent uses of the token 102a because the entity accepting it would be able to verify that the displayed information matched that read by the device used to read the token 102a, e.g., a magnetic card reader.

In some embodiments, value may be exchanged between two Pocket Vaults 102 when one the Pocket Vault 102 generates a token 102a having a value-based or value-linked media stored thereon, and the token 102a so generated is passed to the other the Pocket Vault 102, which then may then access the media and extract value therefrom or add value thereto. As mentioned above, this sort of value exchange may also be accomplished directly between two Pocket Vaults 102 over a wireless network, such as Bluetooth.

As discussed in more detail below, in addition to or in lieu of the token 102a, the Pocket Vault 102 may also generate a bar code for a selected media on the Pocket Vault's display (not shown in Fig. 1), and the bar code reader 107 may be used to scan the displayed bar code to process a transaction. Further, a transaction may be processed via a commercial interface station 104c either by use of a docking terminal or via a wireless network scheme such a Bluetooth. In one embodiment, some commercial interface stations 104c may comprise an interface station linked to a standard commercial

card reader 106 or commercial bar code reader 107, with the card reader 106 or bar code reader 107 being modified to accept input from the station.

Moreover, as is also discussed in more detail below, the Pocket Vault 102 may be configured or programmed to function as an RFID tag that can be used only by an authorized user of the Pocket Vault 102. For example, in response to an interrogation signal from the RFID interrogator 116 (e.g., an interrogator of an automated toll booth), the Pocket Vault 102 (if authorized) can return an appropriate RF signal to authorize payment of the required fee for the toll. In some embodiments, the RFID functionality of the Pocket Vault 102 can be altered by the user so that user is permitted to select the personality of the RFID tag that is embodied by the device. The user may, for example, first use the Pocket Vault 102 as an RFID tag to authorize payment of a toll, and later use the same Pocket Vault 102 as an RFID tag to authorize payment at a service station.

To permit the Pocket Vault holder to select from among the various media stored in memory of the Pocket Vault 102, the Pocket Vault 102 may comprise a display (not shown in Fig. 1). By employing either a display having a user-manipulable touch screen or a separate user input device (not shown in Fig. 1), a Pocket Vault holder can effectively flip through the contents of the Pocket Vault 102 to locate and select a desired media (e.g., a credit card, driver's license, library card, frequent flier card, a particular RFID personality, etc.) much like a person can flip through the contents of his or her wallet to do the same.

The use of a display on the Pocket Vault 102 also creates an opportunity for media providers to go from a static presentation of their brand (logo, etc.) to having the option of dynamic branding and messaging. In addition, using the display, the presentment of active marketing at the "moment of buying decision" is possible. Specifically, the logo and message displayed to the Pocket Vault holder may incorporate motion, moving images and messages. To conserve power, moving images may be presented only at certain times, e.g., in response to internal or external events or communications.

In the embodiment of Fig. 1, the computers 108, 110, and 112, together with the network server 114, may represent a secure infrastructure of server databases capable of storing information for purposes of delivering personalized services to holders of Pocket Vaults 102. The network server 114 may also track activity of Pocket Vault holders and compile marketing information based thereupon that may prove useful to media issuers

and/or advertisers. The Pocket Vault holder may have control over the ability of the network server 114 to track activity. The information maintained on the network system 100 may originate with the holders of Pocket Vaults 102 and/or may originate with the other entities having access to the network system 100 (e.g., advertisers and media issuers).

As discussed below in more detail, in some embodiments of the invention, certain uses of the Pocket Vault 102, as well as each of the interface stations 104a-c, may be permitted only by pre-authorized individuals. To this end, a suitable user authentication technique may be employed in connection with each attempted use of any of these devices. One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis. Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder's identity. In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly.

It should be appreciated that, for some applications, it may be desirable to receive and store authentication information (e.g., fingerprint data) of some or all Pocket Vault holders in the network server 114. Accordingly, in some embodiments, such authentication information may be maintained by the network server 114. This authentication information may be transmitted to the network server 114, for example, when Pocket Vaults 102 are first validated.

As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network

server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information.

A similar level of care may also be taken to ensure that only authorized individuals are permitted to validate interface stations 104a-c by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, as with the Pocket Vaults 102, after it has been confirmed that each interface station's authorization information has been properly stored in the interface station 104, a trust relationship may be set up between the network server 114 and the interface station 104. This relationship may also involve, for example, the registration of a unique encrypted chip ID of the interface station 104 with the network server 114 through a secure Internet connection, the distribution of a digital certificate to the interface station 104, and the grant authority to the interface station 104 to permanently store the interface station operator's authentication information. While, in some embodiments, the Pocket Vault 102 and/or the interface stations 104 are each permitted to store authentication information for only one individual, it should be appreciated that, in alternative embodiments, the Pocket Vault 102 and/or the interface stations 104 may each store authentication information for more than one individual, thereby permitting multiple people to use them.

Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114, as well as with any other networked devices or sites that require a high level of trust. Also, the existence of these trust relationships enable individual Pocket Vaults 102 to accept other services provided by the network servers 114, such as the backup and recovery of information stored within the Pocket Vaults 102. That is, the network servers 114 can serve as a repository for all of the information stored on every validated Pocket Vault 102 (except the holder's authentication information – which, in some embodiments, is stored only in the Pocket Vault 102). To ensure that the network server 114 stores an accurate version of the contents of each Pocket Vault 102, information may, for example, be uploaded from the network server 114 to a Pocket Vault 102 or downloaded from the Pocket Vault 102 to the network server 114 each time the Pocket Vault 102 is interfaced with any of the interface stations 104a-c. Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault

102, and the entire contents of the lost Pocket Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card.

In addition to serving as a repository for Pocket Vault information, the network server 114 may also serve as a repository for information regarding media issuers or advertisers, and may further provide various services to these entities. For example, the network server 114 may facilitate transactions involving media issued by media issuers, and may permit new media to be issued or lost media to be replaced at a fraction of the cost of generating new physical tokens or replacing lost ones. Additionally, the network server 114 may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them. The network server 114 may also function as an advocate for Pocket Vault holders, advertisers, and/or media issuers when it utilizes its portfolio of Pocket Vault holders, media issuers, and/or advertisers to secure privileges. Examples of such advocacy include the ability to secure buying power for Pocket Vault holders as a group or to provide media issuers and advertisers with a highly efficient tool for generating awareness for affinities or causes that fit appropriate holder markets. In sum, the services provided by the network server 114 enable Pocket Vault holders to combine and manage their media data using a single, hand-held device, and enables advertisers and media issuers to understand more about, and more readily reach more of, their customers than ever before.

Fig. 2 shows an example embodiment of the Pocket Vault 102 of Fig. 1. The Pocket Vault 102 may employ components similar to those used in modern personal digital assistants (PDAs) and palm top computers. Examples of such products include PDAs such as the "Palm Pilot" from Palm, Inc. (www.palm.com), and the "Casiopedia" from Casio, Inc. of Dover, New Jersey (www.casio.com). As shown, the Pocket Vault 102 may include a controller 202, as well as a transceiver 204, a user input device 206, a docking interface 208, a read/write memory 210, a write-once memory 212, a power manager 214, an indicator 215, a display 216, a token port 218, and a fingerprint scanner

220, all coupled to the controller 202. In addition, the Pocket Vault 102 may include a hard-wired memory (not shown) to store device serial numbers and key operating system and encryption software components.

Actual views of an example embodiment of the Pocket Vault 102, as well as the token 102a associated therewith, are shown in Figs. 26A-26P. The views of Figs. 26A-P, including the items displayed on the display 216, are discussed in more detail below in connection with the flow diagrams of Figs. 7-12. At this point, however, with reference to Figs. 26A-L and 26O, it may be noted that the Pocket Vault 102 may comprise a housing 2602 in which the components shown in Fig. 2 may be disposed. As illustrated in Figs. 26E and 26F, the housing 2602 may be approximately seventy millimeters wide, approximately one hundred millimeters long, and approximately fifteen millimeters deep. Thus, in the embodiment shown, the housing 2602 has an internal volume of less than 105 cubic centimeters.

Of course, in alternative embodiments, the housing 2602 may be slightly larger or smaller than that shown. For example, in different embodiments, the housing 2602 may have an internal volume of less than five hundred cubic centimeters, or less than four hundred cubic centimeters, or less than three hundred cubic centimeters, or less than two hundred cubic centimeters, or less than one hundred cubic centimeters, or less than any other volume value that falls between one hundred and five hundred centimeters. In one embodiment, the housing 2602 is sized so that the Pocket Vault 102 may readily fit into the rear pocket of a pair of pants. One feature of the illustrative embodiment of the Pocket Vault 102 shown in Fig. 2 which may permit its size to be reduced below that of a standard personal computer is the fact that the embodiment shown lacks a disk drive (either hard or floppy) or any similar memory storage device (e.g., a tape drive) that consumes a significant volume within the housing 2602. It should be appreciated, of course, that alternative embodiments may include such memory devices, and that the invention is not necessarily limited to embodiments that exclude them. In addition to the lack of a disk drive or the like, in some embodiments, the power manager 214 may reduce the power consumption of the active components of the Pocket Vault 102 well below that of a standard personal computer, thereby enabling a very small and light weight battery to be employed, as opposed to the relatively large and heavy batteries typically employed in personal computers.

The housing 2602 may provide a water-resistant or waterproof environment for the components housed thereby. The housing 2602 may further be sealed in a manner suitable to prevent tampering, for example, using a plastic potting compound, and may even be designed such that any attempt to invade the housing 2602 will damage the Pocket Vault 102 such that it may no longer be used. The housing materials of Pocket Vaults 102 may be brightly colored, in addition to traditional black or brown, thereby helping their holders to make a fashion statement and/or permitting them to be readily spotted if misplaced. Deluxe versions may be clad in leather, KevlarTM, GortexTM, aluminum and/or stainless steel. In some embodiments, the housing 2602 may even be woven into garments.

Referring again to Fig. 2, any of a number of devices may be used to implement the controller 202, and the invention is not limited to any particular type of controller. In one illustrative embodiment, for example, the controller 202 comprises a low-power multiprocessor or microcomputer having an on-board SRAM and/or flash memory and a real time clock calendar. One example of a suitable controller is the "Motorola Dragonball" Processor from Motorola, Inc. (www.motorola.com). The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID is released from the Pocket Vault 102 only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder. A signal processor for Bluetooth or another wireless connection may also be employed within or along with the controller 202.

The transceiver 204 may include one or more antennas and may be any type of transceiver (or separate transmitter and receiver) capable of communicating with other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may, in fact, include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface the Pocket Vault with a "docking station" type interface unit, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth. Multiple transceivers (or transmitter/receiver pairs) of the same type may also be employed, if desired.

As discussed in more detail below in connection with Figs. 41 and 42, the transceiver 204 may, for example, serve as the transmitter and receiver of an RFID transponder used to respond to an interrogation signal from an interrogator 116.

In one illustrative embodiment, the user input device 206 is implemented as part of a touch-screen display used as the display 216 (described below). Additionally or alternatively, the user input device 206 may include dedicated buttons, a keypad, a touch pad, a microphone and speech recognition software, a wand or joystick, or any other suitable implement that permits a person to provide input to the controller 202. The user input device 206 may also be integrated into the fingerprint scanner 220 or into an alternative bio-metric input device. By manipulating the user input device 206, a Pocket Vault holder may select one of a number of media stored in memory of the Pocket Vault 102 for display and/or use in connection with a transaction, and may otherwise control or provide input to software executing on the controller 202. In one embodiment, a keypad is employed as the user input device 206, thereby permitting the holder to input a PIN code as a means of authenticating the holder's identity.

The docking interface 208 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 208 may, for example, include a multi-pin plug adapted to mate with a receptacle disposed on the interface units 104a-c, or vice versa. The docking interface 208 may also comprise one or more implements (e.g., grooves or keys) to ensure that the plug or other docking interface 208 mates correctly with the reciprocal device on an interface unit 104 when the two are physically mated together.

The read/write memory 210 may take on any of a number of forms, and the invention is not limited to any particular type of memory. The memory 210 may, for example, comprise a suitable non-volatile SRAM. Similarly, any suitable memory device that permits a only single write operation to take place may be employed as the write-once memory 212. The memory 210 may have instructions stored therein which, when executed by the controller 202, cause the controller 202 to implement the routines/software described below in connection with Figs. 7-12 and/or Fig. 28. Of course, the memory 210 may also contain a suitable operating system (e.g., Palm OS, Microsoft's Windows CE, Microsoft's Windows for Smartcards, or some similar offering), appropriate device drivers, and other software employed in connection with the controller 202 and/or the peripherals thereof. The memory 210 may also be used to store the various media and personal information retained by the Pocket Vault 102. In one illustrative embodiment, the memory 210 stores a plurality of different media issued by different and unrelated media issuers, including both financial (e.g., a credit or debit

card) and non-financial media (e.g., a drivers license or a library card). Other examples of media or information that may be stored in the memory 210 include: a social security card, identification cards, membership cards, discount cards, commuter passes, toll passes, data for various RFID tags, transit cards, access tools such as hotel keys, business cards, coupons, concert and theatre tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipt information, photographs, etc.

As used herein, "financial media" refers to any media which can, as a matter of course, be used to purchase goods or services, whereas "non-financial media" refers to any media which, while possibly having some value to the Pocket Vault holder, cannot, as a matter of course, be used to purchase goods or services. Examples of financial media include value-linked and value-based media such as debit or credit cards issued by a bank or other financial institution, telephone calling cards, etc. Examples of non-financial media include: library cards, driver's licenses, building access cards, etc. In one embodiment, the memory 210 is large enough to store as many as one hundred compressed graphic image files, and full data sets for as many as one hundred types of media.

In addition, the memory 210 may store status information, where useful, for each type of media. Examples of this sort of status information include: information regarding the value remaining on a pre-paid phone card, information regarding an accumulated number of frequent flier miles, information regarding a total number of cups of coffee that have been purchased at a particular coffee shop (e.g., in connection with a buy-ten-get-one-free special), etc. The portion of the memory 210 devoted to memory storage may be divided into three sections: (1) a high-security section, (2) a medium security section, and (3) a non-secure section. The high security section may be used to store value-based or value-linked media such as debit and credit cards and certain ID information such as driver's licenses, passports, building security passes, etc. The medium security section may be used to store low-value, limited use media that may be accessed, for example, by retailers to keep track of frequent purchase credits or the like. The non-secure section may, for example, be used to store notes, membership ID records, emergency contact information, etc. Access to the information included in the various sections may require security or user authentication procedures commensurate with the indicated security level. For example, an accurate fingerprint scan and an

accurate pin code entry may be required to access the high-security section, only an accurate PIN code entry (even by the retailer) may be required to access the medium-security section, and anyone may be permitted to access the non-secure section.

The power manager 214 may comprise any of numerous devices, and the invention is not limited to any particular type of power supply/management device. The power manager may, for example, employ a flat, rechargeable, lithium battery, and associated regulator and power management software. Alternatively, the battery used may be non-rechargeable and/or coin cell-shaped. Solar powered cells may also be a viable option as at least a supplement to battery power, if not a primary source of power for the Pocket Vault 102. This may be made possible because of the typically modest on-time requirements for a Pocket Vault 102. Power management software may also assist in minimizing the power consumption of the Pocket Vault 102. Such software may, for example, invoke an auto-shutdown feature after a preference-set number of seconds, may control the level of screen back-lighting in response to feedback received from a photo-sensor that registers ambient light, and/or may provide battery charge level warnings to Pocket Vault holders.

The indicator 215 may be any device capable of generating a perceptible indication to the holder such as a bell, chime, buzzer, light, vibration, etc., and the invention is not limited to any particular type of device for accomplishing such a result. In one embodiment, for example, the indicator is a chime generator that generates a "chime" sound that can be heard by the Pocket Vault holder.

Any of a number of devices may also be used for the display 216, and the invention is not limited to any particular type of display. As mentioned above, in one embodiment, a touch-screen display may be employed such that at least a portion of the functionality of the user input device 206 may be incorporated therein. Suitable displays may, for example, include any of a black & white, gray-scaled, or color LCD display, or an LCD bi-stable display.

As mentioned above, the use of the display 216, together with the user input device 206 (which may constitute the touch-screen functionality of the display 216) permits the Pocket Vault holder to flip or scroll through the various media stored in the memory 210 in much the same way as a person flips through the contents of his or her wallet. As mentioned above in connection with the description of the indicator 215, in addition to or in lieu of the display 216, other user output devices may also be employed

to provide information to the Pocket Vault holder. For example, light emitting diodes (LEDs), a beeper or buzzer, a speech synthesizer, a vibrator, etc., may be employed in some embodiments of the Pocket Vault 102.

The token port 218 of the Pocket Vault 102 may comprise a cavity or slot in which the token 102a is retained until it is released to be used to engage in a transaction, as well as the hardware employed to secure the token 102a in place when the token 102a has not been authorized to be released. In one embodiment, the token 102a stores a unique (and possibly encrypted) chip ID which is accessible to another device only when the token 102a is successfully released form the token port 218. In addition to the elements described above, the card port 218 may include additional hardware employed in connection with properly generating or configuring the token 102a prior to its release. This hardware is discussed in more detail below in connection with Fig. 6.

The fingerprint scanner 220 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 220 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and from Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner 220 may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is employed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in Fig. 2.

Fig. 3 is a block diagram showing an example embodiment of one of the interface stations 104a-c shown in Fig. 1. The hardware employed to implement each of the stations 104a-c may be identical to the others or may be substantially different,

depending on the environment in which the station 104 is to be used, as well as the functional requirements of the particular station. Therefore, while the example embodiment described herein may be suitable for use as any of the stations, it should be appreciated that each of the stations may, in fact, be configured quite differently than the others.

As shown in Fig. 3, each interface station 104 may include both an the interface station computer 304 and a pocket vault interface unit 302. The interface station computer 304, for example, may be a standard desktop personal computer (PC), and may, as shown, comprise a controller 308, a user input device 318, a memory 320, a modem 322, and a display 324. These components are well known in the art and therefore will not be described in detail herein. The memory 320 of the interface station computer 304 may have instructions stored therein which, when executed by the controller 308, cause the controller to implement the routine described below in connection with Figs. 14-18 as well as any other software, e.g., a browser, drivers, etc., executing on the interface station computer 304.

The pocket vault interface unit 302 is coupled to the interface station computer 304 such that a controller 306 of the pocket vault interface unit 302 can communicate with the controller 308 of the interface station computer 304. The communications interface between these devices may, for example, comprise a Smartcard, Bluetooth or USB interface. As shown, in addition to the controller 306, the pocket vault interface unit 302 may comprise a transceiver 310, a docking interface 312, a finger print scanner 316, a stripe reader 315, and a memory 314. Further, although not shown in Fig. 3, the pocket vault interface unit 302 may also comprise a display and/or another device used to provide feedback to the operator, e.g., an audio indicator or LED.

The stripe reader 315 may be any conventional device for electronically reading the magnetic stripe on a token card such as a credit/debit card or drivers license. The stripe reader 315 may be used, for example, to read information from a token card so that such information can be downloaded to the network server 114 or the Pocket Vault 102.

The memory 314 may be any conventional memory suitable to store the software executed by the controller 306, as well as any data, e.g., stored fingerprint data, used in connection therewith. For example, the memory 314 of the pocket vault interface unit 302 may have instructions stored therein which, when executed by the controller 306,

cause the controller 306 to implement the routine described below in connection with Fig. 13.

As with the transceiver 204 of the Pocket Vault 102, the transceiver 310 of the pocket vault interface unit 302 may be any type of transceiver (or separate transmitter and receiver) capable of communicating with the other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may even include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface the pocket vault interface unit 302 with a Pocket Vault 102, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth.

As with the docking interface 208 of the Pocket Vault 102, the docking interface 312 of the pocket vault interface unit 302 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 312 may, for example, include a multi-pin plug adapted to mate with a receptacle used as the docking interface 208 of a Pocket Vault 102, or vice versa. The docking interface 312 may also comprise one or more implements (e.g., keys or grooves) to ensure that the plug or the like of the docking interface 208 of the Pocket Vault 102 mates correctly with the corresponding implement of the docking interface 312 when the Pocket Vault 102 and pocket vault interface unit 302 are physically mated together.

Finally, as with the fingerprint scanner 220 of the Pocket Vault 102, the fingerprint scanner 316 of the pocket vault interface unit 302 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 316 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and by Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is performed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the interface station operator. For example, some embodiments may employ a charge

coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the operator. Although not shown, the pocket vault interface unit 302 may additionally comprise one or more user input devices enabling the operator to control or provide input to the pocket vault interface unit 302 or the software executing thereon. The fingerprint scanner 316 and/or other bio-metric scanners may, for example, have touch pad capability capabilities built into them, thereby permitting them to constitute such a user input device. Separate user input devices may also be employed.

Fig. 4 shows an example embodiment of the network server 114 shown in Fig. 1. As shown, the network server 114 may comprise one or more controllers 402, as well as a local memory 404, a database 406, and a transceiver 408 coupled thereto. The illustrated components of the network server 114 are well known, and therefore will not be described in detail. The transceiver 408 may, for example, be used to communicate with other devices in the network system 100 (Fig. 1) using a wireless network such as Bluetooth. The controller 404 may also communicate with other network devices via the Internet or a direct connection such as the type established using a dial up modem.

The local memory 404 may have instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement the routines described below in connection with Figs. 19-25 and/or Figs. 30-39. In some embodiments, the local memory 404 and/or database 406 act as a website and execute software which may be accessed by a browser or similar software module operating on a computer. One such embodiment is described below in connection with Figs. 28-39.

The database 406 may, for example, comprise a relational database, and may be used to store the majority, if not all, of the data maintained by the network server 114. The database 406 may, for example, keep a real-time record of critical reference data along with transaction histories, back-up files, and security audit trail information for key events. Examples of specific items that may be stored in the database 406 include: a list of current Pocket Vault holders and appropriate contact information for each; records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304; a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list

of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list; a list of currently authorized locations for interface stations 104 and telephone or other access lines therefor, including business information for each such location and an indication as to the type of interface station 104 it is (e.g., a validation interface station, a personal interface station, or a commercial interface station); a list of currently authorized or registered interface station operators and the interface stations 104 with which they are associated; a list of currently authorized or registered interface stations 104, identified by chip ID and linked to the list of authorized operators therefor, as well as encrypted cookie ID information (if any) for the respective interface stations 104; authorized media data received from media issuers that has not yet been downloaded to individual Pocket Vaults 102; backup data sets for individual Pocket Vault holders; detailed transaction histories for Pocket Vault registrations indicating where each Pocket Vault 102 was shipped from and to, where each Pocket Vault 102 was registered, which authorized interface station operator conducted the registration process, when that authorized operator was added to the list of authorized operators at a particular location, who submitted the key information to add the operator, which corporate representative associated with the network server 114 met with which representative associated with the interface station in establishing each new location for a validation interface station 104a, to whom and when each Pocket Vault 102 was issued; and communication encryption protocols. Each Pocket Vault account defined on the network server 114 may be defined to support multiple Pocket Vaults 102, as well as to identify other family members who may share certain contents of the Pocket Vaults 102 (e.g., family membership in a local museum).

The network server 114 may analyze data regarding consumer transactions, and thereby accumulate demographic information. Using this information, merchants, media issuers, and/or advertisers may, for example, define targeted marketing programs, which the network server 114 may then deliver to Pocket Vault holders that meet particular demographic profiles.

Fig. 5 shows how the memory 210 of the Pocket Vault 102 (Fig. 2) may be organized (conceptually) in accordance with one embodiment of the invention. The purpose of each of the illustrated memory components will be readily understood by those skilled in the art of the invention, and therefore will not be explained in detail.

Fig. 6 is a block diagram showing an example embodiment of the token 102a shown in Figs. 1 and 2. As shown, the token 102 may be equipped with a controller 602. In the embodiment shown, the controller 602 may be selectively programmed, for example, via interface terminals 606 to generate a current in a wire loop 608 so as to generate a magnetic field about the wire loop 608 that simulates a magnetic stripe of a standard credit card-like token. In other words, a magnetic field may be generated along the edge of the token 102a as if a magnetic stripe were present on that edge. The location of the simulated magnetic stripe on the token 102a is identified in Fig. 6 as a virtual magnetic stripe 610.

Appropriate software may be loaded onto the controller 602 (e.g., in an on-board memory of the controller 602) so as to enable the controller to generate the virtual magnetic stripe 610. When the token 102a is disposed in the token port 218, the terminals 606 of the token 102a may engage corresponding terminals of the token port 218, thereby enabling the controller 602 to be programmed appropriately. The programming of the controller 602 may be effected, for example, in response to commands from the controller 202 of the Pocket Vault 102, which commands may be generated in response to software executing on the controller 202.

As shown, the controller 602 may be powered by an appropriate resistor-capacitor (RC) circuit which stores a charge that decays over time. The RC circuit may be initially charged via the terminals 606 when the token 102a is disposed in the token port 218 and the controller 602 is being programmed. After the token 102a is removed from the token port 218, the controller 602 will remain powered only so long as sufficient charge remains stored by the RC circuit 604. Because the controller 602 can generate the virtual magnetic stripe 610 only when it is driven by an adequate power supply, the virtual magnetic stripe will disappear after the charge in the RC circuit 604 has decayed beyond a certain threshold level. Because the decay of an RC circuit is reasonably predictable, the virtual magnetic stripe 610 is disposed on the token 102a only for a finite, predetermined period of time after the token 102a is removed from the token port 218. In one embodiment, after the controller 602 loses power, the information with which it was programmed to enable it to generate the virtual magnetic stripe 610 is also lost. Therefore, the virtual magnetic stripe 610 of the token 102a cannot be used again until the controller 602 is again powered up and reprogrammed. Alternatively, the controller 602 may cut off the power to the wire loop 608 after a preset amount of time

or an amount of time determined by the Pocket Vault holder (possibly within preset limits). Additionally or alternatively, the token 102a may have its own embedded chip ID, which may be accessible only when the token 102a is successfully released form the token port 218.

In some embodiments, the token 102a may possess the characteristics of a bank-issued Smartcard, either in addition to or in lieu of the virtual magnetic stripe 610. Accordingly, the token 102a may include a specialized Smartcard chip or the controller 602 may be programmed to mimic such a chip. In any event, the token 102a may be preloaded with the bank's chip operating system (OS) and possibly customer-specific secure information. In such embodiments, the functionality of the Smartcard components may, for example, be enabled only in response to successful authentication of the Pocket Vault holder, e.g., using the fingerprint scanner 220 of the Pocket Vault 102. Therefore, the customer-specific "Smartcard" information may remain inaccessible so long as the Pocket Vault holder's identity has not been authenticated using the Pocket Vault 102.

In addition to or in lieu of the virtual magnetic stripe 610 and/or Smartcard components described herein, the token 102 may have disposed on it a conventional magnetic stripe that can be selectively written to by a magnetic read/write head in the Pocket Vault 102 before the token 102a is released from the token port 218. Like the other embodiments described above, the programming and/or use of such a token 102a could be restricted until after the identify of the Pocket Vault holder has been verified via biometric authentication, PIN code entry, or otherwise.

Moreover, in some embodiments, the token 102a may also have disposed on it a flexible LCD 612 or other suitable display mechanism or device. Prior to ejection of the token 102a from the token port 218, the Pocket Vault 102 may transfer information to the token 102a (e.g., via terminals 606) for display on the LCD 612. This transfer may either be direct or indirect (e.g., via a separate integrated circuit on the token 102a), and may involve the transfer of alphanumeric information (which may or may not include a hash code) and/or graphics, such as icons or barcodes. This information transferred may be encrypted, and de-encryption may be employed either in the separate integrated circuit on the token 102a or in a processor packaged with the LCD 612. In any event, the LCD 612 may receive the proper data to display, which

would match all or part of the code stored on the card by means of the virtual magnetic stripe 610, a writeable magnetic stripe, Smartcard simulation circuitry, etc.

In some embodiments, the LCD 612 may be powered by a capacitor configured and arranged to drain after a preset time, thereby rendering the LCD 612 inoperable until programmed again by the Pocket Vault 102. Thus, even if the token 102a were still swipeable or otherwise useable, a merchant could opt not to accept it because the requisite authorization information would not longer be displayed for certification purposes.

Instead of or in addition to an LCD or other type of display, some suitable technology may be employed to cause account information, and perhaps other information that is typically embossed or printed on credit cards or Smartcards, to appear temporarily on the token 102a after the token 102a is ejected from the token port 218. One technology that may be appropriate for this purpose is available from E-ink (www.Eink.com).

Thus, when an LCD display, a temporary ink technology, or the like, is employed on the token 102a, not only may the token 102a be selectively configured to have an actual or simulated magnetic stripe (or Smartcard personality) like a typical credit card or Smartcard, but it also may be configured to display information that is typically embossed or printed on such cards, including security enhancing information.

When used by a consumer, retailers may verify authenticity by matching the information displayed on the token 102a with that revealed in the swipe or other token reading process. Without a match, the token 102a may be rejected.

As discussed above, in some embodiments of the Pocket Vault 102, the transceiver 204 (Fig. 2) may be used as the transmitter and receiver of an RFID transponder, and thereby function as an RFID tag. Such an RFID tag may be selectively configured to have one of several personalities and may be rendered operable only when the holder of the Pocket Vault 102 authenticates his or her identity (e.g., in response to an accurate fingerprint scan by fingerprint scanner 220).

To appreciate the manner in which the Pocket Vault 102 may achieve this functionality, a prior art RFID tag system (shown in Fig. 41) will be briefly described. An RFID system includes at least one "RFID tag" and at least one "interrogator." The interrogator communicates with the RFID tag via an RF signal at some suitable frequency, e.g., somewhere between 10 kilohertz and about 5 gigahertz. The distance

between the RFID tag and the interrogator can be as short as near contact or as far as tens of feet away, depending upon the specific technology used. In most applications the RFID tag is a sealed device with no displays or user controls. The interrogator can be a hand held device that is manually operated or can be automated and included in a piece of stationary equipment, for example, at a parking garage, a toll booth, or a service station.

When the RFID tag comes within range of the interrogator, the two devices communicate in a session that may be a one-way read of the RFID tag information by the interrogator, or may be a two-way session in which the interrogator stores information in the RFID tag. The information stored in an RFID tag is typically an identification code such as a serial number. An RFID tag therefore functions much like a bar code, except that it is read by RF. To prevent counterfeiting, the information released from an RFID tag may be signed with a one-way cryptographic key so that it is difficult to decode or duplicate the code.

There are four possible types of RFID tags: (1) active, read only RFID tags, (2) passive, read only RFID tags, (3) active, read/write RFID tags, and (4) passive, read/write RFID tags. Read only RFID tags have information that is stored in them at time of manufacture and can only be read (and not written to) by the interrogator. A Read/Write tag might include a mix of read only information but will have some memory in the tag that can be altered by the interrogator. A passive tag has no battery or other permanent energy source. An active tag, on the other hand, has a battery or is plugged into an external energy source.

An example of a prior art RFID tag 4100 is shown in Fig. 41. As shown, the RFID tag 4100 is a self-contained electronic device that includes a receiver 4102a and a transmitter 4102b that share an antenna 4104 and are connected to a micro-controller 4106. The micro-controller 4106 is further connected to either a read-only memory 4108a or a read/write memory 4108b. The RFID tag 4100 is powered by rectifying the RF energy supplied to the antenna 4104 by the interrogator (not shown). If the RFID tag 4100 were of the "active" type, then an internal battery (not shown) would be employed.

In operation, when the RFID tag 4100 receives an interrogation signal from an interrogator (not shown) via the antenna 4104 and receiver 4102a, the micro-controller 4106 retrieves the tag's serial number from the memory 4108 and passes it to the transmitter 4102b and antenna 4104 for RF transmission to the interrogator. When a

read/write memory 4108b is employed, the micro-controller 4106 may also write information received from the interrogator to that memory.

In addition to typical electronic transponders such as that shown in Fig. 41, there also exist some RFID technologies that use non-electronic RFID tags. For example, interrogators can gather information from some types of RFID tags based solely on some physical property of the tags. For example, each RFID tag may employ several variable length antennas on a dielectric substrate, so that the interrogator can detect the length of the antennas present by sweeping through a range of frequencies. The specific pattern of antennas on the substrate thereby forms a unique code that can be recognized by the interrogator. Yet another approach is to use a surface acoustic wave (SAW) filter in which a surface electrode pattern determines a particular code that can be read by an interrogator.

Once programmed, the prior art RFID tag 4100 performs a single, dedicated function, namely, to release a serial number stored in memory 4108 in response to an interrogation signal, and there exists no control over who can use it for that purpose. In contrast, in some embodiments of the present invention, an RFID tag is provided wherein the personality of the tag, e.g., the code that is released upon interrogation, can be selected by the user from a number of possible personalities, and/or wherein the RFID tag can be rendered operational only by authorized users.

An example embodiment of an RFID tag system 4200 configured in accordance with this aspect of the invention is shown in Fig. 42. As shown, the system 4200 may include an RFID tag 4202 that is identical to the prior art RFID tag 4100, except that memory 4108 of the prior art device has been bypassed or replace by an I/O connection 4204 to the Pocket Vault 102. In such an embodiment, the Pocket Vault 102, rather than the memory 4108, can supply the information to the micro-controller 4106 of the RFID tag 4202 that is to be released to the interrogator (via the transmitter 4102b and antenna 4104) in response to an interrogation signal from the interrogator.

Accordingly, in such an embodiment, the information that is to be released by the RFID tag 4202 in response to an interrogation signal may be controlled by the holder of Pocket Vault 102. The Pocket Vault's holder may therefore select the personality to be taken on by the RFID tag 4202, for example, by using the user input device 206 (Fig. 2) to scroll through various personalities for the RFID tag 4202 that are displayed on the display 216, much like the holder is able to select a desired personality that is to be taken

on by the token 102a. The holder of the Pocket Vault 102 could therefore, for example, at one time select a "FastLane" personality for the RFID tag 4202, enabling the RFID tag to respond to an interrogator at a toll booth, and then at another time select a "Mobile Speedpass" personality, enabling the RFID tag to respond to an interrogator at a Mobile Service Station.

In some embodiments, at least some aspects of the RFID functionality of the Pocket Vault 102 may be exploited only after the identity of the Pocket Vault holder has been authenticated, e.g., using the fingerprint scanner 220 or by proper PIN code entry, thereby providing a level of security for RFID tags that has not heretofore been provided. The Pocket Vault 102 may, of course, permit some non-secure RFID personalities to be taken on by the RFID tag 4202 even without holder authentication.

In some embodiments, the data passed to the RFID tag 4202 can be made to be dependent not just on the recognition of a fingerprint, but based on an actual number tied to a feature extracted from the fingerprint. For example, the area of the finger may be such a feature. The number may then be used as a seed to a cryptographic code generator that creates the data to be sent to the RFID tag 4202.

In the embodiment shown in Fig. 42, the I/O connection 4204 between the Pocket Vault 102 and the RFID tag 4202 may be established in any of a number of ways and the invention is not limited to any particular mechanism or technique for establishing such a connection. In some embodiments, for example, the controller 202 of the Pocket Vault 102 may communicate with the micro-controller 4106 of the RFID tag 4202 via a cable connected between serial or parallel ports on the two devices. Alternatively, the two devices may be directly mated to one another in some suitable manner, or may communicate wirelessly if suitable security precautions are taken. The docking interface 208 of the Pocket Vault 102 may even provide a suitable mechanism for mating the two devices.

In some embodiments, the Pocket Vault 102 may have a separate memory (not shown in Fig. 2) dedicated to the storage of the RFID tag personality that is to be taken on by the RFID tag 4202, and the I/O connection 4204 may give the micro-controller 4106 of the RFID tag 4202 access to that memory. Alternatively, as mentioned above, the personality of the RFID tag 4202 may be communicated directly from the controller 202 of the Pocket Vault 102 to the micro-controller 4106 of the RFID tag 4202 via the I/O connection 4204.

The functionality of the RFID tag 4202 may additionally or alternatively be built directly into the Pocket Vault 102 (Fig. 2), rather that existing as a separate item. In some embodiments, for example, the functionality of the transceiver 4102 and micro-controller 4106 of the RFID tag 4202 may be embodied by the transceiver 204 and the controller 202 of the Pocket Vault 102. Alternatively, the Pocket Vault 102 may include a separate micro-controller, transceiver and/or memory dedicated to the RFID functionality discussed above. In yet another alternative embodiment, the functionality of the RFID tag 4202 may be embodied on the token 102a or on different device that may be selectively released from the housing of the Pocket Vault 102. The token 102a or other releasable device may, for example, include a memory that stores a selected personality for an RFID tag for only a predetermined, finite period of time, and then goes blank.

In some embodiments, the Pocket Vault 102 may also control the content of RFID tags that do not use an electronic circuit. This control can be accomplished in a number of different ways, and the invention is not limited to the use of any particular technique. In one embodiment, for example, the Pocket Vault 102 may activate one or more switches to short out one or more antennas, thereby changing the RFID code represented by them. As with the other embodiments, this selective configuration of an RFID tag may at least in certain circumstances be permitted only after proper authentication of the Pocket Vault holder's identity.

It should be appreciated that the RFID functionality discussed above need not be combined with some or all of the other aspects of the Pocket Vault 102. For example, some embodiments of the invention may comprise simply an RFID tag for which one of several personalities can be selected by the user, and/or an RFID tag that is selectively enabled only following proper user authentication, e.g., using a fingerprint scanner or PIN code entry.

As mentioned above, Figs. 7-12 are flow diagrams illustrating an example implementation of software that may be executed by the controller 202 of the Pocket Vault 102. As described below, this or additional proprietary software may enable menu structures, handle preference management, provide the data on and safeguard the programmability of the virtual magnetic stripe 610 (if so equipped), and ensure proper encryption data management. In one embodiment, local software for each Pocket Vault

102 and pocket vault interface station 104 may be upgraded from time to time by automatic download from the network server 114.

During execution of the routines of Figs. 7-12, various items may be displayed on the display 216, including prompts or icons regarding user input options (when a touch-screen display is employed as the display 216 or a point and click mechanism is employed herewith), and various items may also be displayed on the token 102a when the token 102a is ejected from the token port 218 of the Pocket Vault 102. Figs. 26A-P show examples of how the display 216 and the token 102a may appear as the routines of Figs. 7-12 are executed, and therefore will be discussed in connection with the description of these routines.

Fig. 7 is a flow diagram illustrating an example implementation of a primary routine 700 that may be executed by the controller 202 of the Pocket Vault 102. Instructions for the routine 700 may be stored, for example, in the "applications" section 508 of the memory 210 of the Pocket Vault 102.

As shown, the routine 700 begins at a step 702, wherein it is determined whether the Pocket Vault holder has applied his/her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102. At the step 702, the display 216 of the Pocket Vault 102 may appear as shown in Fig. 26A. That is, the display 216 may be blank at the step 702, as the Pocket Vault 102 is currently powered down.

When, at the step 702, it is determined that the holder has applied his/her fingerprint to the fingerprint scanner 220, the routine 700 proceeds to a step 704, wherein the power manager 214 powers on the Pocket Vault 102. The routine 700 otherwise waits at the step 702 until the Pocket Vault holder has applied a fingerprint to the fingerprint scanner 220. Is should be appreciated, however, that, in some embodiments, the step 702 may not represent an instruction set executed by the processor 202. Instead, the step 702 may represent the detection of the occurrence of a physical action, e.g., the activation of a hardware switch, and the power manager 214 may be activated in response to the detection of such an action, without requiring intervention by the processor 202.

After the step 704, the routine 700 proceeds to a step 706, wherein the fingerprint scanner 220 scans the applied fingerprint of the Pocket Vault holder.

After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. In one embodiment, the

Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of Fig. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114, as described below.

When, at the step 708, it is determined that the Pocket Vault 102 has not yet been validated, the routine 700 proceeds to a step 710, wherein a PROCESS POCKET VAULT VALIDATION routine (described below in connection with Fig. 8) is executed.

When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212.

When, at the step 712, it is determined that the Pocket Vault has not been properly authenticated, the routine 700 proceeds to a step 714, wherein an UNAUTHORIZED HOLDER routine (discussed below in connection with Fig. 9) is executed. Figs. 26B-D show how the display 216 of the Pocket Vault 102 may appear during the UNAUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Fig. 9.

When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device.

In some embodiments, before a Pocket Vault holder is granted access to the contents of his or her Pocket Vault 102, a check may be made to ensure that the components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly, and have not been compromised. Alternatively, the operability and integrity of such components may be checked just prior to their use.

Moreover, in some embodiments, prior to granting a holder access to the contents of the Pocket Vault 102, a check may be made to ensure that the contents of the Pocket Vault 102 have been updated recently. For example, the Pocket Vault 102 may forbid its holder from accessing its contents if the Pocket Vault 102 has not been updated at least

48 hours (or some other specified time period) prior to the attempted use. Updating of the Pocket Vault 102 may be accomplished, for example, using the synchronization or backup and recovery methods described herein.

After the step 713, the routine 700 proceeds to a step 716, wherein it is determined whether the Chameleon Card (i.e., the token 102a) is presently on-board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the card port 218 of Fig. 2).

When, at the step 716, it is determined that the token 102a is not on-board the Pocket Vault 102, the routine 700 proceeds to a step 718, wherein the Pocket Vault holder is informed that the Chameleon Card is not on board, and is asked whether he/she wants to engage in a non-card transaction (i.e., a transaction not involving the token 102a).

After the step 718, the routine 700 proceeds to a step 720, wherein it is determined whether the holder has selected to engage in a non-card transaction.

When, at the step 720, it is determined that the holder has selected not to engage in a non-card transaction, routine 700 returns to the step 716 (described above), wherein it is again determined whether the Chameleon Card is on board the Pocket Vault 102. Therefore, the holder is permitted to engage in a transaction involving the Chameleon Card only when it has been confirmed that the Chameleon Card is on board the Pocket Vault 102.

When, at the step 720, it is determined that the holder has selected to engage in a non-card transaction, the routine 700 proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed.

When, at the step 716, it is determined that the Chameleon Card is on-board the Pocket Vault 102, the routine 700 also proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed. Figs. 26G-N and 26P show how the display 216 of the Pocket Vault 102 and the token 102a ejected therefrom may appear (when employed) during the AUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Figs. 10 and 11.

After each of the steps 710, 714, and 720 (only one of which is executed during each iteration of the routine 700), the routine 700 proceeds to a step 724, wherein the

VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed. Fig. 26O shows how the display 216 of the Pocket Vault 102 may appear during the VERIFY CARD RETURN routine, and therefore is also discussed below in connection with Fig. 12.

After the step 724, the routine 700 proceeds to a step 726, wherein the screen of the display 216 is caused to flash to indicate that the Pocket Vault 102 is being shut down.

After the step 726, the routine 700 proceeds to a step 728, wherein the Pocket Vault 102 is powered down.

After the step 728, the routine 700 returns to the step 702, wherein the Pocket Vault 102 again waits for a fingerprint to be applied to the fingerprint scanner 220, and wherein the display 216 may again appear as shown in Fig. 26A.

Fig. 8 is a flow diagram illustrating an example embodiment of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7 (step 710).

As shown, the routine 710 begins at a step 801, wherein the holder is informed (e.g., on the display 216) that the Pocket Vault 102 is not currently validated, and that the holder must interface the Pocket Vault 102 with an interface unit 302 of an appropriate interface station 104 (e.g., a validation interface station 104a) if the holder desires to validate the Pocket Vault 102.

After the step 801, the routine 710 proceeds to step 802, wherein it is determined whether the Pocket Vault 102 has been interfaced with an appropriate interface unit 302.

When, at the step 802, it is determined that the pocket vault 102 has not yet been interfaced with an appropriate interface unit 302, the routine 710 returns to the step 801 (discussed above).

When, at the step 802, it is determined that the Pocket Vault 102 has been interfaced with an appropriate interface unit 302, the routine 710 proceeds to a step 803, wherein it is determined whether the fingerprint memory, e.g., the write-once memory 212, is empty.

When, at the step 803, it is determined that the fingerprint memory is empty, the routine 710 proceeds to a step 804a, wherein the holder is prompted to apply a fingerprint from one finger of his or her left hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806a – 810a, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After the steps 806a-810a, the routine proceeds to a step 804b, wherein the holder is prompted to apply a fingerprint from one finger of his or her right hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806b – 810b, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After completing the steps 806b-810b, when a total of six fingerprints have been stored in memory, the routine 710 proceeds to a step 812, wherein an encrypted message including the pocket vault ID is transmitted to the interface unit 302, for ultimate transmission to the network server 114.

When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (Fig. 7) matches one of the stored fingerprints.

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does match one of the stored fingerprints, the routine 710 proceeds to the step 812 (discussed above).

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does not match any of the stored fingerprints, the routine 710 proceeds to a step 818, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215) is generated to inform the holder that the validation attempt was unsuccessful.

After the step 818, the routine 710 terminates.

After the step 812, the routine 710 waits at steps 814 and 816 to determine whether an encrypted message including validation information (e.g., a PKI certificate) has been received from the interface unit 302. This encrypted validation information may, for example, be received by the Pocket Vault 102 via either the docking interface 208 or the transceiver 204 of the pocket vault interface unit 302 of a validation interface station 104a. As discussed in more detail below, this encrypted validation information may, for example, be generated by the network server 114 and forwarded to the pocket vault interface unit 302 of a validation interface station 104a (via the interface station

computer 304 of the validation interface station 104a) after certain conditions have been met. The network server 114 may therefore ultimately determine whether each Pocket Vault 102 is permitted to receive this validation information.

When, at the step 816, it is determined that the time-out period has elapsed, the routine 710 proceeds to the step 818 (discussed above).

When, at the step 814, it is determined that encrypted validation information has been received before the timeout period of the step 816 has elapsed, the routine 710 proceeds to a step 820, wherein the validation information is stored in memory.

After the step 820, the routine 710 proceeds to a step 822, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215 of the Pocket Vault 102) is generated to inform the holder that the Pocket Vault 102 has been successfully validated.

After the step 822, the routine 710 terminates.

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7 (step 714).

As shown, the routine 714 begins at a step 902, wherein a menu is displayed on the display 216 that permits the holder to select one of several options: (1) TRY AGAIN, (2) POCKET VAULT RETURN INFORMATION, (3) EMERGENCY INFORMATION, or (4) END SESSION. Fig. 26B shows how the display 216 may appear when the step 902 is reached. As shown, textual information and/or icons representing the various menu options may be displayed to the holder.

After the step 902, the routine 714 proceeds to a step 904, wherein the routine 714 waits for one of the displayed menu items to be selected by the holder (e.g., when the holder touches the location on the screen of the display 216 at which the menu item is displayed).

After one of the menu items has been selected at the step 904, the routine 714 proceeds to a step 906, wherein it is determined whether the TRY AGAIN option was selected. By selecting TRY AGAIN, the holder may request that the holder again be permitted to attempt to access the secure contents of the Pocket Vault 102 by reapplying the holder's fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the user has selected the TRY AGAIN option, the routine 714 proceeds to a step 912, wherein it is determined whether this is

the third sequential time that the scanned fingerprint has failed to match the fingerprint stored in memory.

When, at the step 912, it is determined that three sequential failed matches have occurred, the routine 714 proceeds to a step 914, wherein certain security precautions are taken in light of the multiple failed attempts to match the holder's fingerprint with that stored in the Pocket Vault 102. For example, when multiple failed matches have occurred, the Pocket Vault's secure memory may be erased, a security alert message may be broadcast by the transceiver 204 and/or any other prudent steps may be taken to ensure that an unauthorized user does not access the Pocket Vault's sensitive contents.

After the step 914, the routine 714 terminates.

When, at the step 912, it is determined that this is not the third consecutive time that the holder's fingerprint has failed to match that stored in the Pocket Vault's memory, the routine 714 terminates, and the holder may then again attempt (at the step 702) to access the Pocket Vault 102 by reapplying his/her fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the TRY AGAIN option has not been selected, the routine 714 proceeds to a step 908, wherein it is determined whether there exist any nested menu items for the menu item selected at the step 904.

When, at the step 908, it is determined that nested menu items do exist for the selected menu item, the routine 714 proceeds to a step 910, wherein the nested menu items for the selected menu item are displayed to the holder on the display 216.

After the step 910, the routine 714 returns to the step 904, wherein the routine 714 again waits for the holder to select one of the displayed menu items.

When, at the step 908, it is determined that no nested menu items exist for the selected menu item, the routine 714 proceeds to a step 916, wherein it is determined whether the END SESSION option has been selected.

When, at the step 916, it is determined that the END SESSION option has been selected, the routine 714 terminates.

When, at the step 916, it is determined that the END SESSION option has not been selected, the routine 714 proceeds to a step 918, wherein the information, if any, for the selected menu item is displayed to the holder on the display 216. Because the step 918 is reached only after a failed attempt to match the holder's fingerprint with that stored in the memory of the Pocket Vault 102, the information displayed at the step 918

may, for example, include information as to where the Pocket Vault 102 may be returned if it is found by someone other than the Pocket Vault holder (see Fig. 26C), or may be emergency information regarding the holder such as the holder's blood type, allergies, persons to contact in case of an emergency, etc. (see Fig. 26D). It should be appreciated that any of a number of non-secure media may be selected using the menu access routine discussed above in connection with steps 904-910, and may be displayed to the person accessing the Pocket Vault 102, regardless of the identity of that person. Of course, this non-secure information may be information that the holder would not mind falling into the hands of a stranger should the holder misplace or have his/her Pocket Vault 102 stolen.

After the step 918, the routine 714 proceeds to a step 920, wherein after a delay of a certain period of time (e.g., thirty seconds), the holder is prompted to reapply his/her fingerprint within a particular period of time (e.g., ten seconds) to avoid shut down of the Pocket Vault 102.

After the step 920, the routine 714 proceeds to a step 922, wherein it is determined whether a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds.

When, at the step 922, it is determined that a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 returns to the step 918 (discussed above), wherein the selected information is again displayed to the user.

When, at the step 922, it is determined that a fingerprint has not been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 terminates.

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine of Fig. 7 (step 722).

As shown, the routine 722 begins at a step 1002, wherein it is determined whether an advertisement is scheduled for display on the Pocket Vault 102. Information regarding whether certain advertisements are to be displayed by the Pocket Vault 102 may have been uploaded, for example, from the personal interface station 104b in response to the holder previously interfacing the Pocket Vault 102 with the personal interface station 104b to synchronize the contents of the Pocket Vault 102 with information stored on the network server 114. The advertiser 108 (Fig. 1) may, for example, have made arrangements with the company operating the network server 114 to

have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b.

When, at the step 1002, it is determined that an advertisement has been scheduled, the routine 722 proceeds to a step 1004, wherein the scheduled advertisement is displayed, for example, for approximately two seconds. Fig. 26I shows an example of how the display 216 may appear when such an advertisement is displayed.

After the step 1004, the routine 722 proceeds to a step 1006, wherein a "welcome screen" is displayed for a brief period (e.g., one second). Fig. 26G shows an example of how the display 216 may appear when such a welcome screen is displayed.

When, at the step 1002, it is determined that an advertisement is not scheduled, the routine 722 proceeds immediately to the step 1006, and no advertisement is displayed to the Pocket Vault holder.

After the step 1006, the routine 722 proceeds to a step 1008, wherein it is determined whether a "preferred" menu has been selected or pre-set for initial display to the Pocket Vault holder.

When, at the step 1008, it is determined that a preferred menu has been selected or pre-set, the routine 722 proceeds to a step 1012, wherein the display 216 fades to the preferred menu. Figs. 26H and 26J show examples of how the display 216 may appear when such a preferred menu is displayed. In the example of Fig. 26H, the preferred menu immediately shows the holder's preferred credit card as the selected menu item. Should the holder opt to use this media to engage in a transaction, the holder can simply choose the media directly. Alternatively, the holder may opt to access the HOME menu or other menu items by selecting appropriate icons displayed on the screen. In the example of Fig. 26J, the preferred menu immediately shows, perhaps, a selected group of the holder's most frequently used menu items.

When, at the step 1008, it is determined that a preferred menu has not been selected or pre-set, the routine 722 proceeds to a step 1010, wherein the display 216 fades to a standard HOME menu of secure items. Fig. 26L shows an example of how the display 216 may appear when the HOME menu is displayed.

After either one of the steps 1010 and 1012 has been executed, the routine 722 proceeds to a step 1014, wherein the routine 722 waits for the holder to select one of the displayed menu items.

When, at the step 1014, it is determined that the holder has selected a particular menu item, the routine 722 proceeds to a step 1016, wherein it is determined whether the holder has selected to enter or return to the HOME menu.

When, at the step 1016, it is determined that the holder has selected the HOME option, the routine 722 proceeds to the step 1010, wherein the HOME menu of secure items is displayed.

When, at the step 1016, it is determined that the holder has selected a menu item other than the HOME option, the routine 722 proceeds to a step 1018, wherein it is determined whether there exist any nested menu items for the selected menu item.

When, at the step 1018, it is determined that nested menu items do exist for the selected menu item, the routine 722 proceeds to a step 1020, wherein the nested menu items for the selected menu item are displayed. Thus, the holder may work his/her way through various layers of menu items until the desired menu item is reached. It should be appreciated that the menu items on the higher-level layers therefore may be categorized so as to enable the holder to quickly reach the desired media or other menu option.

When, at the step 1018, it is determined that no nested menu items exist for the selected menu item, the routine 722 proceeds to a step 1022, wherein it is determined whether the holder has selected a media from among the available menu items.

When, at the step 1022, it is determined that the holder has not selected a media, the routine 722 proceeds to a step 1040, wherein information relating to the selected non-media item may be displayed, or some other function may performed in accordance with the holder's selection. A non-media menu selection may involve, for example, preference settings for certain functional aspects of the Pocket Vault 102, e.g., whether the holder has a preferred secure menu (see step 1008). Preferences for the services or the device can be selected and, as appropriate, distributed to the Pocket Vault 102 either on the spot or the next time the Pocket Vault 102 is interfaced with an appropriate interface station 104. Preferences may, for example, include definition of home pages, connection of secure and non-secure media, order of media presentment, sort orders, user interface options, synchronization defaults, etc. Preferences that determine which items are displayed on the home page or on other pages may be defined. For example, a Pocket Vault holder may set up three preference sets: one for "business," one for "personal," and one for "vacation." The "personal" and "business" preference sets may

be set to be effective at different times of the day and/or different days of the week. The "vacation" preference set may be made effective for specific blocks of time determined by the Pocket Vault holder, possibly overriding the normal timing of the "personal" and "business" sets. The Pocket Vault holder may choose to establish the various preference settings based on his or her judgment or he or she may choose to allow the network server 114, supported by various databases, knowledge of the Pocket vault holder's various media and goals set by the Pocket Vault holder (e.g., minimize interest cost on credit cards or maximize frequent flyer miles, etc.), to determine optimal media use patterns and resulting media menu contents for a particular Pocket Vault holder. Preferences may also be defined between media that will link them for: (a) affiliate credits (like frequent flyer miles) that may be automatically presented to a merchant and tracked for a holder, (b) available discounts afforded by a membership (like senior citizen or AAA discounts), and/or (c) process improvement purposes (e.g., when information needs to be presented in a certain order to work properly). For example, a linkage preference may facilitate presentation of a discount card before presentation of a payment card when buying groceries.

After the step 1040, the routine 722 proceeds to a step 1042, wherein the holder is prompted either to END the session, or to return to the HOME menu.

After the step 1042, the routine 722 proceeds to a step 1044, wherein it is determined whether the holder has opted to END the session or to return to the HOME menu.

When, at the step 1044, it is determined that the holder has selected to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1044, it is determined that the holder has opted to END the session, the routine 722 terminates.

When, at the step 1022, it is determined that the holder has selected a media from the displayed menu items, the routine 722 proceeds to a step 1024, wherein the selected media is displayed to the holder on the display 216. The selected media may, for example, be a particular credit card, in which case the name of the credit card and/or the logo for the credit card and any preferred advertisement, specials, etc., for the selected media may be displayed to the holder as well.

After the step 1024, the routine 722 proceeds to a step 1026, wherein the holder is prompted to choose to: (1) EJECT the card, (2) to invoke a WIRELESS transaction, or (3) to return to the HOME menu.

After the step 1026, the routine 722 proceeds to a step 1028, wherein it is determined which of these three options has been selected by the holder.

When, at the step 1028, it is determined that the holder has opted to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1028, it is determined that the holder has selected the EJECT card option, the routine 722 proceeds to a step 1032, wherein it is determined whether the Chameleon Card is on board the Pocket Vault 102 (i.e., whether the token 102a is disposed in the token port 218).

When, at the step 1032, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 722 proceeds to a step 1034, wherein the holder is informed that the Chameleon Card is not on board the Pocket Vault 102.

After the step 1034, the routine 722 proceeds to the step 1026 (discussed above).

When, at the step 1032, it is determined that the Chameleon Card is on board the Pocket Vault 102, the routine 722 proceeds to a step 1036, wherein the PROCESS CARD TRANSACTION routine (discussed below in connection with Fig. 11) is executed.

After the step 1036, the routine 722 proceeds to a step 1038, wherein the VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed.

After the step 1038, the routine 722 proceeds to the step 1042 (discussed above).

When, at the step 1028, it is determined that the holder has opted to invoke a wireless transaction, the routine 722 proceeds to a step 1030, wherein the wireless transaction involving the selected media is executed. This wireless transaction may be invoked, for example, using the transceiver 204 of the Pocket Vault 102 to communicate with the transceiver 310 (Fig. 3) of a commercial interface station 104c (Fig. 1) over a wireless network, such as Bluetooth. Alternatively, the selected wireless transaction may be an RFID transaction if an RFID personality has been selected from amongst the available media. If such an RFID transaction has been selected, an appropriate RFID code may be supplied to the controller responsible for broadcasting an RF signal containing that code in response to an interrogation signal. If that controller is on the

Chameleon card, then these steps may alternatively be performed in connection with the PROCESS CARD TRANSACTION routine (step1036) discussed below.

As mentioned above, in embodiments that permit wireless transactions, a check of the wireless components may be made (e.g., verifying that an internal antenna (not shown) is in place and connected, and that related circuitry is not defeated or compromised in any way), prior to granting the holder access to the contents of the Pocket Vault 102. Alternatively, such a check may be made in response to such a wireless transaction being requested, e.g., at the step 1030.

After the step 1030, the routine 722 proceeds to the step 1042 (discussed above).

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine of Fig. 10 (step 1036).

As shown, the routine 1036 begins at a step 1102, wherein the Chameleon Card is configured to carry the selected media, and is ejected from the card port 218 (Fig. 2). As discussed above, the token 102a may be configured to carry the selected media in any of a number of ways, and the invention is not limited to any particular type of configuration technique. The card may be configured, for example, by using a magnetic read/write head to write to a conventional magnetic stripe on the token 102a, by causing the token 102a to generate a simulated magnetic stripe, by causing the token 102a to have a bar code disposed on it, and/or simply by causing a card number and perhaps security-related information to be visibly displayed it (e.g., using an LCD display or some type of printing technique). The token 102a may possibly be configured to hold such information for only a predetermined, finite period of time, so that it is not useable after such time. It should be appreciated, of course, that the card need not be temporarily configured in all embodiments, and may alternatively be configured in a more permanent manner in some embodiments.

After the step 1102, the routine 1036 proceeds to a step 1104, wherein the selected media is grayed out on the display 216 to indicate that the media is currently in use by the Chameleon Card. When the selected media is grayed out, the Pocket Vault's ability to configure another Chameleon Card with the grayed out media may also be disabled. Therefore, in such an embodiment, even if the Pocket Vault holder had an additional Chameleon Card available, the Pocket Vault 102 would be incapable of loading that media onto that Chameleon Card.

After the step 1104, the routine 1036 proceeds to a step 1106, wherein it is determined whether the selected media has stored value associated with it. The selected media may, for example, represent a pre-paid calling card from which value is deducted each time the media is used in a particular transaction, or a frequent flier card to which value (e.g., miles) is added in connection with each airline ticket purchased.

When, at the step 1106, it is determined that the selected media does have stored value associated with it, the routine 1036 proceeds to a step 1108, wherein a "stored value flag" (discussed below in connection with step 1126 of routine 1036 (Fig. 11) and step 1212 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1108, the routine 1036 proceeds to a step 1110, wherein it is determined whether the holder has set a default option so as to permit the holder to maintain expense records by recording transactions into registers assigned to expense categories.

When, at the step 1106, it is determined that the selected media does not have stored value associated with it, the routine 1036 proceeds immediately to the step 1110.

When, at the step 1110, it is determined that the holder has not opted for the ability to maintain expense records, the routine 1036 terminates.

When, at the step 1110, it is determined that the holder has opted for the ability to maintain expense records, the routine 1036 proceeds to a step 1112, wherein the holder is prompted to decide whether to record the currently-pending transaction.

After the step 1112, the routine 1036 proceeds to a step 1114, wherein it is determined whether the holder has opted to record the pending transaction.

When, at the step 1114, it is determined that the holder has not opted to record the transaction, the routine 1036 terminates.

When, at the step 1114, it is determined that the holder has opted to record the transaction, the routine 1036 proceeds to a step 1116, wherein a menu including a number of options involving expense categories are displayed to the holder on the display 216.

After the step 1116, the routine 1036 proceeds to a step 1118, wherein the routine 1036 waits for the holder to select one of the displayed menu options.

When, at the step 1118, it is determined that the holder has selected a menu item, the routine 1036 proceeds to a step 1120, wherein it is determined whether the holder

selected the SKIP RECORD option, e.g., when the holder has changed his or her mind and opted not to record a particular transaction.

When, at the step 1120, it is determined that the holder has selected the SKIP RECORD option, the routine 1036 terminates.

When, at the step 1120, it is determined that holder has not selected the SKIP RECORD option, the routine 1036 proceeds to a step 1122, wherein it is determined whether any nested menu items exist for the selected menu item.

When, at the step 1122, it is determined that nested menu items do exist for the selected menu item, the routine 1036 proceeds to a step 1124, wherein the nested menu items are displayed to the holder on the display 216.

After the step 1124, the routine 1036 returns to the step 1118 (discussed above).

When, at the step 1122, it is determined that no nested menu items exist for the selected menu item, the routine 1036 proceeds to a step 1126, wherein it is determined whether the stored value flag was set to TRUE at the step 1108 (discussed above).

When, at the step 1126, it is determined that the stored value flag is set to TRUE, the routine 1036 proceeds to a step 1128, wherein a "record stored value transaction" flag (discussed below in connection with step 1216 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1128, the routine 1036 terminates.

When, at the step 1126, it is determined that the "stored value" flag is not TRUE, the routine 1036 proceeds to a step 1130, wherein the holder is prompted to enter a dollar amount to be recorded for the transaction.

After the step 1130, the routine 1036 proceeds to a step 1132, wherein the routine 1036 waits for the holder to enter a transaction amount. After the holder has entered a transaction amount, the routine 1036 proceeds to a step 1134, wherein a "transaction summary approval" menu is displayed to the holder on the display 216. In the example shown, this menu permits the holder to select (1) to APPROVE the recordation, (2) to change the expense CATEGORY for the transaction, or (3) to change the AMOUNT to be recorded.

After the step 1134, the routine 1036 proceeds to a step 1136, wherein it is determined which of the menu items displayed in step 1134 the holder has selected.

When, at the step 1136, it is determined that the holder has selected to change the transaction AMOUNT, the routine 1036 returns to the step 1130 (discussed above).

When, at the step 1136, it is determined that the holder has opted to change the expense CATEGORY, the routine 1036 returns to the step 1116 (discussed above).

When, at the step 1132, it is determined that the holder has opted to APPROVE the recordation, the routine 1036 proceeds to a step 1138, wherein the entered transaction amount is added to the expense register for the selected category, and the balances associated therewith are updated accordingly.

After the step 1138, the routine 1036 terminates.

Fig. 12 is a flow diagram illustrating the VERIFY CARD RETURN routine of Fig. 7 (step 724).

As shown, the routine 724 begins at a step 1202, wherein it is determined whether the Chameleon Card is currently on board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the token port 218).

When, at the step 1202, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 724 proceeds to a step 1204, wherein the holder is prompted to return the Chameleon Card to the token port 218 (see Fig. 260).

After the step 1204, the routine 724 proceeds to a step 1206, wherein it is determined whether a timeout period (e.g., ten seconds) has elapsed since the user was last prompted to return the Chameleon Card to the token port 218.

When, at the step 1206, it is determined that the timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1206, it is determined that the timeout period has elapsed, the routine 724 proceeds to a step 1208, wherein the user is again prompted to return the Chameleon Card, this time with an audio indication (e.g., a "chime" sound generated by the indicator 215 of Fig. 2).

After the step 1208, the routine 724 proceeds to a step 1210, wherein it is determined whether an extended timeout period (e.g., 10 minutes) has elapsed since the user was first prompted to return the Chameleon Card to the token port 218.

When, at the step 1210, it is determined that the extended timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1210, it is determined that the extended timeout period has elapsed, the routine 724 terminates.

When, at the step 1202, it is determined that the Chameleon Card is on board the Pocket Vault 102 (i.e., the token 102a is disposed within the token port 218), the routine

724 proceeds to a step 1212, wherein it is determined whether the "stored value" flag was set to TRUE in step 1108 of the routine 1036 (Fig. 11).

When, at the step 1212, it is determined that the "stored value" flag is not TRUE, the routine 724 terminates.

When, at the step 1212, it is determined that the "stored value" flag is TRUE, the routine 724 proceeds to a step 1214, wherein the stored value for the selected media is updated based on the amount deducted from the Chameleon Card during its use.

After the step 1214, the routine 724 proceeds to a step 1216, wherein it is determined whether the "record stored value transaction" flag was set to TRUE in the step 1128 of the routine 1036 (Fig. 11).

When, at the step 1216, it is determined that the "record stored value transaction" flag is FALSE, the routine 724 proceeds to a step 1222, wherein the "stored value" flag is set to FALSE.

When, at the step 1216, it is determined that the "record stored value transaction" flag is TRUE, the routine 724 proceeds to a step 1218, wherein the dollar amount of the transaction is added to the selected expense register (i.e., the expense register selected at the step 1118 of the routine 1036 (Fig. 11)). The dollar amount entered is determined based on the dollar amount that was deducted from the stored value on the Chameleon Card as a result of the transaction.

After the step 1218, the routine 724 proceeds to a step 1220, wherein the "record stored value transaction" flag is set to FALSE.

After the step 1220, the routine 724 proceeds to the step 1222 (discussed above)

After the step 1222, the routine 724 terminates.

In addition to a routine such as that discussed above in connection with Figs. 7-12, certain software enhancements may also be disposed in the memory 210 of a Pocket Vault 102 for use with the controller 202. One such software enhancement involves the use of "system preference file" software. This software may establish certain preferences that cannot be altered on the Pocket Vault 102 by the holder, and which may be stored in encrypted form, along with certain information regarding value-based media. For example, Pocket Vaults 102 may be sold with a choice of two or three advertising profiles. During the Pocket Vault registration and validation process (described below), an encrypted system preference file may be created that indicates whether the device was, for example, subject to a "Premium," "Plus" or "Base" profile status. This status

may have been selected, for example, on the Pocket Vault 102 itself, or using one of the interface stations 104a-c when the Pocket Vault 102 was interfaced therewith.

Under the "Premium" profile, the Pocket Vault 102 may be advertising-free, but cost a significant amount. Under the "Plus" profile, the Pocket Vault 102 may display only advertising related to shops or services you currently patronize, but cost significantly less than the "Premium" version. Under the "Base" profile, the Pocket Vault 102 may have a variety of advertising on a regular basis, subject only to network "saturation effectiveness" limitations, and the Pocket Vault 102 may be free, or nearly so (e.g., a small purchase charge to generate in-store revenue for the retailer may be charged).

A holder's choice about participation in specific promotional campaigns linked to the holder's buying behavior may also be part of the registration process and affect retail pricing. Once chosen, the network server 114 may send a message to the Pocket Vault 102, e.g., via the validation interface station 104a, and direct the storage of necessary encrypted information on the Pocket Vault 102 (e.g., "Buyer Profile Participant").

The advertising and marketing choices may be changed at a date after purchase and result in a changed set of costs (either credits or debits) to the Pocket Vault holder. Other system preference data may include the "saturation effectiveness" limitations on the amount of advertising that can appear during any given single use window (a particular period during which the device is powered on), any given hour, any given day and/or any given month. The limitations may control both the number of advertisements permitted and the amounts of advertisement time permissible (e.g., seconds per advertisement), by category (e.g., such limitations may, for example, based on categories of advertisements be imposed general advertising, advertising from retailers that the Pocket Vault holder already patronizes and advisory notices from the network server 114. For example, these limits may be set to balance the need for advertising revenue with the need to not overwhelm or annoy Pocket Vault holders. This preference file may, for example, limit all advertising to one advertisement per "on-session," two advertisements per hour, four advertisements per day and/or twenty advertisements per month. General advertisements might get priority claim on this time up to a set limit (say 75% of all advertisement time), with targeted advertisements next, and advisory messages last.

Another software enhancement that may be employed is software used for preference file management. Such "preference file management" software may, for example, include a default file which is periodically updated from the network server 114, and a Pocket Vault holder custom file. Using this software, the holder may, for example, be able to modify: (1) the initial on-screen backdrop and message greeting; (2) the menu structure and media order within menu screens; (3) some (but not all) of the bio-metric input requirement parameters; (4) the amount of on-time after the bio-metric data is confirmed (within pre-set limits); (5) the ability to conceal all or part of the credit or debit account information on the Chameleon Card display area; (6) the normal restaurant tip percentage; (7) the links between certain media; and/or oversight preference restrictions.

For example, some of the menu tree structures for the Pocket Vault 102 may be set by the holder. This may include the sequence in which certain screens appear (e.g., debit screens before credit screens), among credit screens (e.g., Visa before MasterCard) and media order-of-appearance within a screen (e.g., FirstCard Visa before ChaseVisa).

Generally, a retailer does not need to see a credit or debit account number, while the approving entity contacted on the dialup modem does. Today, credit and debit cards have this information embossed on the card and recorded in the magnetic stripe on the back of the card. If the magnetically encoded information is unreadable due to mechanical wear of the magnetic stripe or for other reasons, the embossed image can always be read by the clerk and manually keyed in. There is no way for this embossing to disappear when it is not needed and appear at just the right time, either with a standard card or a Smartcard. As a result, such numbers are generally in view and this visibility may lead to fraud. In one embodiment, the Pocket Vault 102 may be programmed to conceal this number, unless prompted to the contrary by the holder. A retailer may confirm the kind of credit or debit being presented and the full name on the card, without having to see or be told the account number. On the rare occasion when the number itself is needed, the holder may, for example, repeat the bio-metric input to the Pocket Vault 102 to reveal the card account number. If placed in the personal interface station 104c, such account numbers may be automatically revealed (e.g., through detection of an encrypted cookie on the interface station computer 304 of the personal interface station 104c).

If the holder establishes a preferred tip percentage, this preferred tip amount may be automatically applied to restaurant checks. This may eliminate a step in restaurant check close-out and reduce the hassle of calculating an appropriate tip and eliminate the need for waitstaff to return to pick up the credit receipt with the tip.

The holder may also choose to link certain media on the Pocket Vault 102 to reduce selection tasks at the point-of-transaction. For example, the holder may link certain credit or debit cards to certain frequent buyer ID cards, thereby enabling the holder to pick a grocery store frequent buyer card (which would be linked to a debit card and brought up automatically after the grocery store card).

At the point of registration or issuance, a Pocket Vault holder may be asked if there is to be any transaction oversight security. If the answer is yes, a second bio-metric input may be required from the individual endowed with that oversight role. For example, a parent may choose to get a Pocket Vault 102 for a child or other relative who may lack certain fiscal discipline. At issuance, and prior to any credit or debit media being added to the Pocket Vault 102, the oversight authority may need to be established. The person having such oversight authority may then have sole access to a profile of transaction preference data. The person having the oversight authority may therefore create and modify this profile any time after issuance. This data set may limit one or more of the following: (1) debit and credit transaction dollar volume per day, per week and/or per month; (2) certain purchase restrictions such as the types of retailers to whom payments are permitted, such as exclusion of gambling establishments or liquor stores; and (3) geographic restrictions such as payments within 10 miles of a son's or daughter's college campus, but not beyond).

Another software enhancement that may be employed is software for managing media image libraries. Every media image sent to the display 216 may actually be a composite of from two to five layers of graphics files. Layers one, two and four may, for example, be stored in media library files while layers three and five may include text and data files stored in memory on the Pocket Vault 102. For example, a credit card image may comprise separate layers for: (1) the standard credit card background and icon; (2) the issuing bank's overlay icons and text; (3) the individual's account number; and (4) customized advertising from the issuing bank and/or credit card company.

Layering the image in this fashion may minimize data transmission requirements, reduce memory storage requirements, and speed up screen display. For example, Pocket

Vaults 102 may be preloaded at point of manufacture with background images of the top ten credit images, three passport images (e.g., EU, US, Japan), and a handful of other globally-relevant backgrounds. When, for example, a Pocket Vault holder living in Boston initially registers a device, it may trigger downloading of the top five additional background images prevalent in that area. When the individual applies for and is electronically issued a new credit card over the network system 100, the download from the network server 114 may include a second layer credit card company overlay for the credit card, along with the third layer of account and name information, and the fourth layer of the most recent customized advertisement from the credit card company related to a seasonal promotion of card usage.

The advertisement layer may be temporary in nature. This layer may, for example, remain on-screen for a given number of seconds, predetermined by the time period of the advertisement paid for by the advertiser. Underneath such an advertisement, a fifth layer of Pocket Vault holder-determined data may appear, also for a temporary period, in this case for privacy reasons and for a period set by the holder. This positioning of the holder's data below the advertising data increase the value of the advertisement time, since holders will be likely to view the display 216 awaiting the appearance of their data, which may also remain on-screen for only a set number of second. For example, such holder-specific data may include the last date of the next billing period, or the total charges since the last billing period on this particular card or on all of the holder's credit cards. Such balance information may be generated, for example, by the financial management software. The initial on-screen image may also be layered, for example, with a market-tailored backdrop and a sign-on message, both of which possibly being modifiable could be modified by the appropriate setting of user preferences.

Another software enhancement that may be employed is software to manage memos. Certain screen choices may, for example, result in the viewing of memos created by and for the Pocket Vault holder. These memos may be written on a home PC and transferred to a Pocket Vault 102 when the Pocket Vault 102 is interfaced with the personal interface station 104c for an update/download session. Alternatively, such memos may be created on the Pocket Vault 102 using a screen-based keyboard function similar to that of a Palm Pilot. The memo template software may provide certain

standard backgrounds and layouts to support this feature. This feature may help to eliminate the need for scraps of various notes now found in most wallets.

Yet another software enhancement that may be employed is software to manage advertising messages. Such advertising message management software may, for example, perform several noteworthy functions: (1) limiting the appearance of advertising in accordance with the advertising profile (e.g., stored in the network server 114) of the particular Pocket Vault holder; (2) limiting the appearance of advertising to a certain number of times per on-session, per hour, per day, per week and/or per month; (3) tracking the number of times each advertisement appears since the last download/update session (since the number of on-sessions during any period will govern the number of opportunities certain advertisements have to run, this tracking may be necessary to enable billing of advertisers for actual advertisement exposure levels; (4) generating reminder advertisements for frequent buyer cards (e.g., a message such as "Ten weeks since your last car wash! One more and the next is free!"); and (5) tracking the effectiveness of advertising through linkage to the transaction files (e.g., the ability to build more accurate, comprehensive buying profiles since all of an individual's media are now "under one roof").

Another software enhancement that may be employed is software to process transaction data. Such transaction processing software may, for example, include the ability to track total outstanding transactions on particular media and compare those to media limits at the time of the next transaction, along with date validity of the media. If a particular piece of media is no longer valid, selection of this item from a menu may produce a message such as "expired," or "requires update to extend period of validity," or "payment of balance required before re-use."

Another software enhancement that may be employed is software to manage frequent buyer data. Such frequent buyer data management software may, for example, track purchases at stores with frequent buying programs that participate in the network system 100. This software may also indicate any frequent buyer credits that are about to expire or create advertisements that remind their Pocket Vault holders that they are about to qualify for a free item. For example, a tenth gasoline purchase at a service station/car wash may generate a message indicating that the holder is "now entitled to free car wash."

Yet another software enhancement that may be employed is software for managing financial information. This type of software may, for example, enable easy download advertisements into personal finance software used by some PC owners. It may also support certain on-board functionality in the Pocket Vault, such as charge card management, automatically shifting from the preferred credit card to another credit card, for example: (1) when a transaction would cause a credit limit to be exceeded, (2) when using a different card would lengthen the time after which actual payment would be due, (3) when using another card would garner desired contest eligibility, or maximize cash back points for a particular period, and/or (4) when use of another card would preclude having to pay annual dues.

Another software enhancement that may be employed is Global Positioning Software. Integration of this functionality with memo information and frequent buyer information may induce visits to nearby stores at convenient times to take advantage of sales, frequent buyer credits, etc.

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine 1300 that may be executed by the controller 306 of the pocket vault interface unit 302 (Fig. 3).

As shown, the routine 1300 begins at a step 1346, wherein it is determined whether a card has been swiped through the stripe reader 315 of the interface unit 302.

When, at the step 1346, it is determined that a card has been swiped, the routine 1300 proceeds to a step 1348, wherein information from the swiped card read by the stripe reader 315 is transmitted to the interface station computer 304.

After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match).

When, at the step 1346, it is determined that a card has not been swiped, the routine 1300 proceeds directly to the step 1302 (discussed above).

When, at the step 1302, it is determined that such a first encrypted message has not been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1338, wherein it is determined whether any encrypted information and/or commands have been received from the interface station computer 304.

When, at the step 1338, it is determined that information and/or commands have been received from the interface station computer 304, the routine 1300 proceeds to a step 1340, wherein the received information and/or commands are forwarded to the Pocket Vault 102.

After the step 1340, the routine 1330 proceeds to a step 1342, wherein it is determined whether any information and/or commands have been received from the Pocket Vault 102.

When, at the step 1338, it is determined that no information or commands have been received from the interface station computer 304, the routine 1300 proceeds directly to the step 1342 (discussed above).

When, at the step 1342, it is determined that information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1344, wherein the received information and/or commands are forwarded to the interface station computer 304.

After the step 1344, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1342, it is determined that no information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds directly to the step 1346.

When, at the step 1302, it is determined that a first encrypted message including a Pocket Vault ID has been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1304, wherein the first encrypted message is forwarded to the interface station computer 304 (Fig. 3).

After the step 1304, the routine 1300 proceeds to steps 1306 and 1308, wherein it is determined whether a fingerprint has been scanned by the fingerprint scanner 316 of the pocket vault interface unit 302 before a timeout period measured by the step 1308 has elapsed.

When, at the steps 1306 and 1308, it is determined that a fingerprint has not been scanned within the timeout period of step 1308, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302.

When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304.

After the step 1312, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1310, it is determined that the scanned fingerprint does not match any fingerprint stored in the memory 314 of the pocket vault interface unit 302, the routine 1300 proceeds to a step 1314, wherein a message is transmitted to the interface station computer 304 indicating there has been an unsuccessful attempt to authenticate an operator of the pocket vault interface unit 302.

After the step 1314, the routine 1300 proceeds to steps 1316 and 1318, wherein it is determined whether, before the expiration of a timeout period measured by the step 1318, a request has been received from the interface station computer 304 to add a new operator to the pocket vault interface unit 302.

When, at the steps 1316 and 1318, it is determined that such a request has not been received from the interface station computer 304 in a timely manner, the routine 1300 returns to the step 1302 (discussed above).

When, at the steps 1316 and 1318, it is determined that a request to add a new operator to the pocket vault interface unit 302 has been received from the interface station computer 304 in a timely manner, the routine 1300 proceeds to steps 1320 and 1322.

At the steps 1320 and 1322, it is determined whether three identical fingerprints have been stored in the interface unit 302 for each of the operator's two hands before the expiration of a timeout period measured by the step 1322. The operator may be prompted, e.g., on the display 324 of the interface station computer 304, to take appropriate steps to ensure his or her fingerprints are properly scanned. An example routine for obtaining the requisite fingerprint data from a user is discussed above in connection with steps 804a-810a and 804b-810b (for the Pocket Vault 102), and therefore will not be repeated here.

When, at the steps 1320 and 1322, it is determined that the requisite fingerprint information has not been stored in a timely manner, the routine 1300 proceeds to a step

1336, wherein an indication (e.g., a message or an audio tone) regarding the unsuccessful new operator validation attempt is generated.

After the step 1336, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1320 and 1322, it is determined that the fingerprint information has been successfully stored in the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1324, wherein an encrypted message including an ID unique to the interface unit 302 is transmitted to the interface station computer 304 for ultimate registration with the network server 114.

After the step 1324, the routine 1300 proceeds to step 1326 and 1328, wherein is determined whether a message including validation information (e.g., a PKI certificate for the interface unit 302) has been received from the network server 114 (via the interface station computer 304) before the expiration of a timeout period.

When, at the steps 1326 and 1328, the validation information is not received by the interface unit 302 in a timely manner, the routine 1300 proceeds to the step 1336 (discussed above).

When, at the steps 1326 and 1328, it is determined that the validation information is received by the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1330, wherein the validation information is stored for the new operator.

After the step 1330, the routine 1300 proceeds to a step 1332, wherein an indication (e.g., a message or an audio tone) regarding the successful validation of the new operator is generated.

After the step 1332, the routine 1300 returns to the step 1346 (discussed above).

Fig. 14 is a flow diagram illustrating example implementation of a primary routine 1400 that may be executed by the controller 308 of the interface station computer 304 of Fig. 3.

As shown, the routine 1400 begins at a step 1402, wherein a menu is displayed on the display 324 of the interface station computer 304 that gives the operator of the interface station computer 304 several options to choose from. These options may, for example, include: (1) the option to request that a Pocket Vault 102 be validated (i.e., permitted to store a new finger print), (2) the option to request that the information currently stored on a Pocket Vault 102 be updated (e.g., information may be uploaded from the network server 114), (3) the option to request that a transaction involving a

Pocket Vault 102 be authorized, and/or (4) the option to access a website on the network server 114 and take advantage of the functionality thereof.

It should be appreciated that the foregoing are only examples of menu options that may be provided to the operator of the interface station computer 304, and that the invention is not limited to the particular examples described. It should also be appreciated that fewer than all of the options shown may be provided in connection with different types of interface stations. For example, a validation interface station 104a may be provided only with option (1), a personal interface station may be provided only with option (2), and a commercial interface station may be provided only with option (3). In many instances, option (4) may be the only option required or desired to be employed by the user, as the website may itself provide all of the functionality of the other options (1)-(3). If fact, in such circumstances, the user need not be provided with a menu at all, as the user could simply log on the website using a browser. An embodiment of a network system in which a website may be accessed by a server in this manner is discussed below in connection with Figs. 28-39.

After displaying the menu at the step 1402, the routine 1400 proceeds to a step 1404, wherein it is determined whether any requests to validate Pocket Vaults 102 have been received.

When, at the step 1404, it is determined that no request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1408, wherein it is determined whether any requests to update information on Pocket Vaults 102 have been received.

When, at the step 1408, it is determined that no request to update the information on a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1412, wherein it is determined whether any requests to authorize transactions involving Pocket Vaults 102 have been received.

When, at the step 1412, it is determined that no request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1416, wherein it is determined whether the interface station computer has received any messages from Pocket Vault interface units 302 indicating that an unsuccessful operator authentication has occurred (i.e., the fingerprint of an operator scanned by the fingerprint scanner 316 has failed to match a fingerprint stored in the memory 314).

When, at the step 1416, it is determined that no such messages have been received, the routine 1400 proceeds to a step 1420, wherein it is determined whether a request to access a website on the network server 114 has been received.

When at the step 1420, it is determined that no request to access the website on the network server 114 has been received, the routine 1400 returns to the step 1402, wherein the menu of the various options for the operator is again displayed. Thus, the menu 1402 is displayed until one of the various options is selected in accordance with any of the steps 1404, 1408, 1412, 1416, or 1420.

When, at the step 1404, it is determined that a request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1406, wherein the PROCESS REQUEST TO VALIDATE POCKET VAULT routine (discussed below in connection with Fig. 15) is executed.

After the step 1406, the routine 1400 proceeds to the step 1408 (discussed above).

When, at the step 1408, it is determined that a request to update the information on a Pocket Vault 102 has been received, the routine 1410 proceeds to a step 1410, wherein the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine (discussed below in connection with Fig. 16) is executed.

After the step 1410, the routine 1400 proceeds to the step 1412 (discussed above).

When, at the step 1412, it is determined that a request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1414, wherein the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine (discussed below in connection with Fig. 17) is executed.

After the routine 1414, the routine 1400 proceeds to the step 1416 (discussed above).

When, at the step 1416, it is determined that a message has been received from an the interface station computer 304 indicating that an attempted fingerprint match of an operator has failed, the routine 1400 proceeds to a step 1418, wherein the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine (discussed below in connection with Fig. 18) is executed.

After the routine 1418, the routine 1400 proceeds to the step 1420 (discussed above).

When, at the step 1420, it is determined that a request to access a website on the network server 114 has been received, the routine 1400 proceeds to a step 1422, wherein

the PROCESS REQUEST TO ACCESS WEBSITE routine (discussed below in connection with Figs. 30-39) is executed.

After the step 1422, the routine 1400 returns to the step 1402 (discussed above).

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine of Fig. 14 (step 1406).

As shown, the routine 1406 begins at a step 1502, wherein the potential new Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302. This may be accomplished, for example, by interfacing the docking interface 208 of the Pocket Vault 102 with the docking interface 312 of the pocket vault interface unit 302.

After the step 1502, the routine 1406 proceeds to steps 1504 and 1506, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1506.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that an error has occurred in the Pocket Vault validation process.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1506, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1506, the routine 1406 proceeds to steps 1508 and 1510, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1510.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to the step

1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1526, the routine 1406 terminates.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1512, wherein the interface station operator is prompted to input information regarding the new Pocket Vault holder into the interface station computer 304.

After the step 1512, the routine 1406 proceeds to a step 1514, whereat the routine 1406 waits until all of the requisite information regarding the new Pocket Vault holder has been entered properly (e.g., via the user input device 318 of the interface station computer 304).

After the step 1514, the routine 1406 proceeds to a step 1516, wherein the network server 114 (Fig. 1) is contacted.

After the step 1516, the routine 1406 proceeds to a step 1518, wherein the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with a request that the new Pocket Vault holder be validated.

After the step 1518, the routine 1406 proceeds to steps 1520 and 1522, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1522.

When, at the steps 1520 and 1522, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1524, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1520 and 1522, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1528, wherein, in an encrypted format, the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1528, the routine 1406 proceeds to steps 1530 and 1532, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1532, and prior to receiving a message from the network server 114 indicating that the request to validate the new Pocket Vault holder has been denied.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, or it is determined that a message has been received indicating that the request to validate the new Pocket Vault holder has been denied, the routine 1406 proceeds to a step 1538, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was unsuccessful.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine 1406 proceeds to a step 1534, wherein the encrypted validation information (e.g., a PKI certificate) from the network server 114 is forwarded to the pocket vault interface unit 302 for forwarding on to the Pocket Vault 102.

After the step 1534, the routine 1406 proceeds to a step 1536, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was successful. In addition to this message, when the pocket vault interface unit 302 forwards this message on to the Pocket Vault 102, the Pocket Vault 102 itself may provide, for example, an audio indication such as a chime, indicating that the Pocket Vault 102 has been successfully validated.

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine of Fig. 14 (step 1410).

As shown, the routine 1410 begins at a step 1602, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302.

After the step 1602, the routine 1410 proceeds to steps 1604 and 1606, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1606.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1634, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1606, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1606, the routine 1410 proceeds to steps 1608 and 1610, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1610.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to the step 1634, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1634, the routine 1410 terminates.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1612, wherein the network server 114 is contacted.

After the step 1612, the routine 1410 proceeds to a step 1614, wherein a request to update the information on the Pocket Vault 102 is transmitted to the network server 114.

After the step 1614, the routine 1410 proceeds to steps 1616 and 1618, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1618.

When, at the steps 1616 and 1618, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1620, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1616 and 1618, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1622, wherein, in an encrypted manner, the interface station operator ID, the interface unit ID, and the Pocket Vault ID are transmitted to the network server 114.

After the step 1622, the routine 1410 proceeds to steps 1624 and 1626, wherein it is determined whether encrypted updates have been received from the network server 114 for loading onto the Pocket Vault 102 prior to the expiration of a timeout period measured by the step 1620, and prior to the network server 114 denying the requested attempt to upload information.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have been received in a timely manner, the routine 1410 proceed to a step 1630, wherein the received updates are transmitted to the pocket vault interface unit 302 so that they may be subsequently forwarded to the Pocket Vault 102 for uploading thereto.

After the step 1630, the routine 1410 proceeds to a step 1632, wherein a message is displayed to the holder indicating that the requested updates have been successfully uploaded to the Pocket Vault 102.

After the step 1632, the routine 1410 terminates.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have not been received from the network server 114 in a timely manner, or that the network server 114 has denied the request to upload information onto the Pocket Vault 102, the routine 1410 proceeds to a step 1628, wherein a message is displayed on the display 324 indicating that the attempt to update the information on the Pocket Vault 102 was unsuccessful.

After the step 1628, the routine 1410 terminates.

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine of Fig. 14 (step 1414).

As shown, the routine 1414 begins at a step 1702, wherein the operator of the interface station computer 304 is prompted to input information regarding the proposed transaction involving the Pocket Vault 102.

After the step 1702, the routine 1414 waits at a step 1704 until all of the information regarding the requested transaction has been entered.

After, at the step 1704, it is determined that all of information regarding the requested transaction has been entered, the routine 1414 proceeds to a step 1706, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault with the pocket vault interface unit 302.

After the step 1706, the routine 1414 proceeds to steps 1708 and 1710, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1710.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1726, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1712, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1712, the routine 1414 proceeds to steps 1714 and 1715, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1715.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to the step 1726, wherein a message is displayed on the display 324 of the interface station

computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1726, the routine 1414 terminates.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1716, wherein the network server 114 is contacted.

After the step 1716, the routine 1414 proceeds to a step 1718, wherein the request regarding the proposed transaction involving the Pocket Vault 102 is transmitted to the network server 114.

After the step 1718, the routine 1414 proceeds to step 1720 and 1722, wherein it is determined whether the transaction request has been acknowledged by the network server 114 before the expiration of a timeout period measured by the step 1722.

When, at the steps 1720 and 1722, it is determined that the request has not been acknowledged in a timely manner, the routine 1414 proceeds to a step 1724, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

After the steps 1724, the routine 1414 terminates.

When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732.

When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed.

When , at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has been received in a timely manner, the routine 1414 proceeds to a step 1734, wherein a message is forwarded to the pocket vault interface unit 302 indicating that the requested transaction has been approved. This message may also be used to update information on the Pocket Vault 102, and/or to cause the Pocket Vault 102 to generate an indication (e.g., an audio tone) that the transaction has been approved.

After the step 1734, the routine proceeds to a step 1738, wherein a message is displayed on the display 324 indicating that the requested transaction has been approved.

After the step 1738, the routine 1414 terminates.

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine of Fig. 14 (step 1418).

As shown, the routine 1418 begins at a step 1802, wherein the operator of the interface station computer 304 is informed that the attempted use the pocket vault interface unit 302 (when the operator applied his or her finger print to the fingerprint scanner 316) was not authorized.

After the step 1802, the routine 1418 proceeds to a step 1804, wherein the operator is prompted to either: (1) add a NEW OPERATOR to the interface unit 302, or (2) ABORT the attempt to use the interface unit 302.

When, at the step 1806, it is determined that the operator has chosen to ABORT the attempt to use the interface unit 302, the routine 1418 terminates.

When, at the step 1806, it is determined that the operator has chosen to add a NEW OPERATOR, the routine 1418 proceeds to a step 1808, wherein a message is transmitted to the pocket vault interface unit 302 indicating the operator's desire to add a new operator to the pocket vault interface unit 302.

After the step 1808, the routine 1418 proceeds to a step 1810, wherein the operator is prompted to input information regarding the proposed new operator into the interface station computer 304 (e.g., using the user input device 318), and is provided with instructions as to the application of three identical fingerprints from each of his or her two hands to the fingerprint scanner 316 of the interface unit 302.

After the step 1810, the routine 1418 proceeds to a step 1812 wherein the routine 1418 waits until all of the requisite information regarding the proposed new interface station operator has been entered properly.

When, at the step 1812, it is determined that all of the requisite information regarding the proposed new operator has been entered properly, the routine 1418 proceeds to a step 1814, wherein the network server 114 is contacted.

After the step 1814, the routine 1418 proceeds to a step 1816, wherein the request to add the new operator to the pocket vault interface unit 302 is transmitted to the network server 114.

After the step 1816, the routine 1418 proceeds to steps 1818 and 1820, wherein it is determined whether the request by the interface station computer has been acknowledged by the network server 114 prior to the expiration of a timeout period measured by the step 1820.

When, at the steps 1818 and 1820, it is determined that the request has not been acknowledged in a timely manner, the routine 1418 proceeds to the step 1822, wherein a transmission failure message is displayed.

After the step 1822, routine 1418 terminates.

When, at the steps 1818 and 1820, it is determined that the request has been acknowledged in a timely manner, the routine 1418 proceeds to the step 1824, wherein a message, including the information regarding the proposed new operator and the interface unit ID, is transmitted to the network server 114 in an encrypted manner.

After the step 1824, the routine 1418 proceeds to steps 1826 and 1828, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1828, and prior to the network server 114 denying the addition of the new interface station operator.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine 1418 proceeds to a step 1830, wherein the encrypted validation information (e.g., a PKI certificate) is forwarded from the interface station computer 304 to the pocket vault interface unit 302.

After the step 1830, the routine 1418 proceeds to a step 1834, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was successful.

After the step 1834, the routine 1418 terminates.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, the routine 1418 proceeds to a step 1832, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was unsuccessful.

After the step 1832, routine 1418 terminates.

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine 1900 that may be executed by the network server 114 of Fig. 1.

As shown, the routine 1900 may begin at a step 1902, wherein it is determined whether any requests have been received to register new Pocket Vault holders.

When, at the step 1902, it is determined that a request has been received to register a new Pocket Vault holder, the routine 1900 proceeds to a step 1904, wherein the request to register the new Pocket Vault holder is processed. An example of a routine that may be employed to implement the step 1904 is discussed in more detail below in connection with Fig. 20.

When, at the step 1902, it is determined that no request to register a new Pocket Vault holder has been received, the routine 1900 proceeds to a step 1906, wherein consumer marketing information is compiled and transmitted to subscribing media issuers and advertisers.

After the step 1906, the routine 1900 proceeds to a step 1908, wherein it is determined whether any requests from media issuers or advertisers have been received to update the network server 114.

According to one aspect of the invention, media issuers and advertisers may have the option to utilize the functionality of the network server 114 to update the account characteristics of authenticated Pocket Vault holders. These updates may, for example, be delivered from the computers 108, 110, and 112 to a secure location within the database 406. When each selected holder next synchronizes with network server 114 (e.g., as described below in connection with routine 1914 of Fig. 22), any media characteristics updated by the media issuers or advertisers may be uploaded to that holder's the Pocket Vault 102. The database of account updates may be revised periodically based on the media issuer's systems (e.g., pursuant to the routine 1910 of Fig. 21 - described below). Confirmation of the update process may be provided to the issuer after a synchronization session is complete for a particular Pocket Vault holder (see step 2206 of routine 1914 (Fig. 22) below).

When, at the step 1908, it is determined that a request to update the network server 114 has been received from a media issuer or advertiser, the routine 1900 proceeds to a step 1910, wherein the request from the media issuer or advertiser is processed. An example of a routine that may be employed to implement the step 1910 is discussed in more detail below in connection with Fig. 21.

When, at the step 1908, it is determined that no request from a media issuer or advertiser to update the network server 114 has been received, the routine 1900 proceeds to a step 1912, wherein it is determined whether any requests have been received from holders to update information on their Pocket Vaults.

When, at the step 1912, it is determined that such a request has been received, the routine 1900 proceeds to a step 1914, wherein the request to update the Pocket Vault information is processed. An example of a routine that may be employed to implement the step 1914 is described in more detail below in connection with Fig. 22.

When, at the step 1912, it is determined that no request from a holder to update information on a Pocket Vault 102 has been received, the routine 1900 proceeds to a step 1916, wherein it is determined whether any holders have requested that new files be loaded onto the network server 114.

When, at the step 1916, it is determined that a holder has requested that a new file be loaded onto the network server 114, the routine 1900 proceeds to a step 1918, wherein the holder's request to load the new file onto the network server 114 is processed. An example of a routine that may be employed to implement the step 1918 is described in more detail below in connection with Fig. 23.

When, at the step 1916, it is determined that no request by a holder to load a file onto the network server 114 has been received, the routine 1900 proceeds to a step 1920, wherein it is determined whether any requests have been made to authorize transactions. Such a request may be made, for example, by a merchant operating a commercial interface station 104c. In this regard, it should be appreciated that, when a token 102a is employed to engage in a transaction with a commercial card reader 106 or a commercial bar code reader 107, a request for transaction approval may not be made to the network server 114. Instead such a transaction approval request may be made through conventional, existing communication and approval channels for such devices. Therefore, it should be understood that the step 1922 is generally reached only when it is possible for the network server 114 to check the identity of the Pocket Vault holder, the

identity of the Pocket Vault 102, and possibly identity of the operator of a commercial interface station, based on communications with the Pocket Vault 102 (e.g., via a commercial interface station 104c or via a wireless network such as Bluetooth).

When, at the step 1920, it is determined that a request to authorize a transaction has been made, routine 1900 proceeds to a step 1922, wherein the request to authorize the transaction is processed. An example of a routine that may be employed to implement the step 1922 is discussed in more detail below in connection with Fig. 24.

When, at the step 1920, it is determined no request to authorize a transaction has been made, the routine 1900 returns to the step 1902 (discussed above). With regard to the routine 1900 of Fig. 19, it should be appreciated that all of the requests to accomplish the various tasks may be placed in a queue so that they are serviced on a first-come, first-served or any other basis, rather than servicing them in the particular order shown in Fig. 19.

Fig. 20 is a flow-diagram illustrating an example of a routine that may be employed to implement the step 1904 of the routine 1900 (Fig. 1).

As shown, the routine 1904 begins at a step 2002, wherein a request received from the interface station computer 304 to register a new Pocket Vault holder is acknowledged, and the network server 114 requests the interface station computer 304 to transfer the relevant information regarding the proposed new holder to the network server 114.

After the step 2002, the routine 1904 proceeds to a step 2004, wherein the routine 1904 waits for all of the requisite holder registration information to be received from the interface station computer 304.

When, at the step 2004, it is determined that all of the requisite holder registration information has been received from the interface station computer 304, the routine 1904 proceeds to a step 2006, wherein it is determined whether the proposed Pocket Vault use is authorized. An example of a routine that may be employed to implement the step 2006 is discussed below in connection with Fig. 25. In determining whether a particular Pocket Vault use is authorized, there are numerous parameters which may be checked. For example, the port to which the interface station computer is connected (e.g., the telephone number or IP address of the computer) may be checked to ensure that it is authorized. Additionally, information from the interface station computer 304 (e.g., a "cookie") may be checked to ensure that the computer itself has been registered with the

system. Further, it can be checked whether the current operator of the interface station computer 304 is registered as being associated with the interface station computer 304 being used, and that the proposed new Pocket Vault holder is authorized to use that particular the Pocket Vault 102. In sum, the identity of (1) each piece of equipment, (2) each operator of each piece of equipment, and (3) each location of each piece of equipment may be checked to ensure that the particular use of the Pocket Vault is authorized. It should be appreciated fewer than all of these parameters, different parameters, and/or additional parameters can be checked in alternative embodiments of the invention, and that the invention is not limited to embodiments wherein all of the aforementioned parameters are checked to verify that a particular Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1904 terminates. In such a situation, it is also possible to generate some sort of security alert message to put someone or some entity on notice that an unauthorized use of a Pocket Vault has occurred.

When, the routine 2006 has determined that the proposed Pocket Vault use is authorized, the routine 1904 proceeds to a step 2008, wherein all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114 (Fig. 4). As shown in Fig. 20, this information may include, for example, the interface station operator ID, the interface unit ID, the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder.

After the step 2008, the routine 1904 proceeds to a step 2010, wherein the network server 114 transmits encrypted validation information to the interface station computer 304, which then may be passed on to the pocket vault interface unit 302, and then to the Pocket Vault 102, so as to enable the new holder's fingerprint to be stored in the memory of the Pocket Vault 102.

After the step 2010, the routine 1904 terminates.

Fig. 21 is a flow diagram illustrating example of a routine that may be employed to implement the step 1910 of the primary routine 1900 (Fig. 19).

As shown, the routine 1910 begins at a step 2102, wherein it is determined whether all of the requested updates have been received from the media issuer or advertiser.

When, at the step 2102, it has been determined that all of the requested updates have been received, the routine 1910 proceeds to a step 2104, wherein it is determined whether the media issuer or advertiser is authorized access to the network server 114. This authorization process may require some sort of authentication of the identity of the computer used by the media issuer or advertiser requesting the update, the operator of the computer, and/or the location of the computer, in a manner similar to that in which the interface stations 104 and their operators are authorized.

When, at the step 2104, it is determined that the media issuer or advertiser is not authorized access to the network server 114, the routine 1900 proceeds to a step 2106, wherein a message is transmitted to the media issuer or advertiser informing the media issuer or advertiser that access to the network server 114 has been denied.

After the step 2106, the routine 1910 terminates.

When, at the step 2104, it is determined that the media issuer or advertiser is authorized access to the network server 114, the routine 1910 proceeds to a step 2108, wherein the updates received from the media issuer or advertiser are logged onto the network server 114.

After the step 2108, the routine 1910 terminates.

Fig. 22 is a flow diagram illustrating an example a routine that may be employed to implement the step 1914 of the primary routine 1900 (Fig. 19).

As shown, the routine 1914 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1914 terminates.

When, at the step 2006, it is determined that the Pocket Vault use is authorized, the routine 1914 proceeds to a step 2202, wherein encrypted updates are transmitted to the interface station computer 304 for loading onto the Pocket Vault 102.

After the step 2202, the routine 1914 proceeds to steps 2204 and 2206, wherein the time and date of the updates are logged (step 2204), and the media issuers or advertisers are informed that the updates have been made (step 2206).

Fig. 23 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1918 of the primary routine 1900 (Fig. 9).

As shown, the routine 1918 begins at a step 2302, wherein it is determined whether the file to be loaded onto the network server 114 relates to a secure media issuer.

When, at the step 2302, it is determined that the file does not relate to a secure media issuer, the routine 1918 proceeds to a step 2304, wherein the network server 114 is updated with the non-secure file.

After the step 2304, the routine 1918 terminates.

When, at the step 2302, it is determined that the to-be-loaded file does relate to a secure media issuer, the routine 1918 proceeds to a step 2306, wherein it is determined whether the secure media issuer is a Pocket Vault participant (i.e., a media issuer having access to the network server 114).

When, at the step 2306, it is determined that the secure media issuer is not a Pocket Vault participant, the routine 1918 proceeds to a step 2308, wherein an advisory is sent to the holder indicating an inability to load the file, and inquiring as to whether the holder desires to load the file in a non-secure format. The holder may, for example, opt to load the file to the network server 114 in such a way that the content of the file is not encodable to the Chameleon Card, but can be displayed and shown to a POS operator and manually keyed in at POS by the POS operator.

After the step 2308, the routine 1918 proceeds to a step 2316, wherein it is determine whether the holder has elected to load the file in a non-secure format.

When, at the step 2316, it is determined that the holder has elected not to load the file in a non-secure format, the routine 1918 terminates.

When, at the step 2316, it is determined that the holder has elected to load the file in a non-secure format, the routine 1918 proceeds to a step 2318, wherein the file is loaded onto the network server 114 in a non-secure format.

After the step 2318, the routine 1918 terminates.

When, at the step 2306, it is determined that the secure media issuer is a Pocket Vault participant, the routine 1918 proceeds to a step 2310, wherein the media issuer is queried as to the account status of the holder.

After the step 2310, the routine 1918 proceeds to a step 2312, wherein it is determined whether authorization has been received from the media issuer to load the file.

When, at the step 2312, it is determined that authorization has not been received from the media issuer, the routine 1918 proceeds to the step 2308 (discussed above).

When, at the step 2312, it is determined that authorization has been received from the media issuer, the routine 1918 proceeds to a step 2314, wherein the network server 114 is updated with the secure file.

After the step 2314, the routine 1918 terminates.

Fig. 24 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1922 of the primary routine 1900 (Fig. 19).

As shown, the routine 1922 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted use of the Pocket Vault 102 is authorized.

When, at the step 2006, it is determined that the attempted Pocket Vault use is not authorized, the routine 1922 terminates.

When , at the step 2006, it is determined that the attempted Pocket Vault used is authorized, the routine 1922 proceeds to a step 2402, wherein it is determined whether the requested transaction is within acceptable account parameters (e.g., as set by the media issuer).

When, at the step 2402, it is determined that the requested transaction is not within acceptable account parameters, the routine 1922 proceeds to a step 2404, wherein a message is transmitted to the entity that requested the transaction (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107) indicating that the transaction is outside of acceptable account parameters.

After the step 2404, the routine 1922 terminates.

When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (Fig. 4). As shown, the logged information may include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction.

After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).

After the step 2408, the routine 1922 terminates.

Fig. 25 is a flow diagram illustrating an example of a routine that may employed to implement the step 2006 of the routines 1904 (Fig. 20), 1914 (Fig. 22), and 1922 (Fig. 24).

As shown, the routine 2006 begins at a step 2502, wherein it is determined whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source (e.g., an authorized telephone line or an authorized internet protocol (IP) address).

When, at the step 2502, it is determined that the entity proposing the transaction is not connected to a valid source, the routine 2006 proceeds to a step 2510, wherein the transaction is refused, and a security alert is generated so that appropriate action(s) may be taken.

When, at the step 2502, it is determined that the entity proposing the transaction is connected to a valid source, the routine 2006 proceeds to a step 2504, wherein it is determined whether the ID of the interface station, card reader, barcode reader or RFID interrogator is valid, and is properly linked to the source to which is connected.

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is not valid, the routine proceeds to the step 2510 (discussed above).

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation.

When, at the step 2506, it is determined that the Pocket Vault ID (when available and required) is not valid, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the Pocket Vault ID (if available) is linked to the ID of the entity proposing the transaction, e.g., a commercial interface station 104c, a card reader 106, a barcode reader 107, or an RFID interrogator 107.

When, at the step 2508, it is determined that the ID of the Pocket Vault 102 (when available) is not linked to the ID of the entity proposing the transaction, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2508, it is determined that the Pocket Vault ID is linked to the ID of the entity proposing the transaction, or that the ID of the Pocket Vault is not required, the routine 2006 proceeds to a step 2512, wherein the Pocket Vault use is authorized.

With regard to the information checked in connection with the routine 2006 to determine whether a particular Pocket Vault use is authorized, it should be appreciated that, in some embodiments, fewer than all of the verification steps discussed above may be performed when lesser degrees of security are desired or required. For example, in some embodiments, there may be no restrictions as to who can operate an interface station, the source to which the station is connected, and/or the ID of the station.

Figure 27 illustrates a network system similar to that described hereinabove. The system of Fig. 27, however, includes several additional components which serve to increase the network's functionality and utility. Accordingly, it should be appreciated that, in addition to the components illustrated in Fig. 27, the system may also include all or some of the components and features of the system described above in connection with Figs. 1-26, and may also incorporate all or some of that system's functionality.

As shown in Fig. 27, the Pocket Vault 102 may be coupled to an interface station 104 (including an interface unit 302 coupled to an the interface station computer 304). The interface unit 302 may include a communication port 2706, which is adapted to perform basic communications functions for interaction between the interface unit 302 and each of the Pocket Vault 102 and the interface station computer 304. This communication can take place over physical wires using a USB protocol or HotWire, or any other suitable protocol. Alternatively, the communication can be wireless, using a standard wireless protocol, such as Bluetooth, or any other suitable protocol. The communication port 2706 may, of course, be adapted to perform communications functions depending on the requirements on the particular protocol used. In an example embodiment, a USB protocol is used, and the interface unit 302 is connected to the interface station computer 304 through a USB port. Several suitable methods/techniques for interfacing the Pocket Vault 102 with the interface unit 302 are described above.

In addition to the communication port 2706, as in the embodiment described above, the interface unit 302 contains a stripe reader 315. The purpose and operation of the stripe reader 315 is described below in connection with Figure 34.

The interface station computer 304 may be any suitable computer that employs one or more processors to execute instructions stored in memory. The interface station computer 304 may even comprise several inter-networked computers.

In the illustrative embodiment shown, the interface station computer 304 may use the communication software 2710 to communicate with the network server 114 via the network 2724. The communication software 2710 may be any of a number of communication programs known in the art, and the invention is not limited to any particular type of software. The software 2710 may, for example, comprise a web browser, a terminal emulation program, a proprietary program, or any other software module capable of communicating with other computers using the network 2724. The network 2724 may be any communication network known in the art. For example, the network 2724 may comprise the World Wide Web, a Local Area Network, or any other networking arrangement adapted for communication between digital computers.

In the embodiment shown, the communication software 2710 uses internet settings 2722 when accessing the network 2724. The internet settings 2710 may include any user preferences or software settings relevant to communication functions and usability of the communication software 2710. The internet settings 2722 may comprise, for example, the network name and the identification of the interface station computer 304, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The communication software 2710 may access the network 2724 through communication protocol layer 2714. Depending on how the interface station computer 304 is physically connected to the network 2724. The communication protocol layer 2714 may be dial-up software, a TCP/IP layer, or any other suitable networking layer. The communication protocol layer 2714 may, for example, execute low-level communication functions, thereby providing useful abstractions to the communication software 2710. In an example embodiment, the interface station computer 304 is connected to the network 2724 using a modem, and the communication protocol layer 2714 is a dialup software module.

As shown, the interface station computer 304 may also contain one or more communication drivers 2712. Although multiple drivers may, in fact, be employed, for simplicity of discussion, the description hereinafter may refer to all such drivers as a single "driver." The communication driver 2712 acts both as a device driver for the interface unit 302, and also as a communications driver capable of accessing internet settings 2722 and facilitating communications between the Pocket Vault 102 and the server 114 by using the communication protocol layer 2714 to establish a connection to the network server 114 through the network 2724.

The network server 114 may comprise any suitable processor-based device or its equivalent. It may be either a single or multi-processor machine, or even a collection of servers inter-networked together. In one embodiment, the network server 114 stores both data and applications that are accessible to users. The network server 114 may, for example, store and serve a website, i.e., a collection of web pages and data that are available to users via a browser.

The network server 114 may include one or more controllers 402 and a database 406, as described above in connection with Figure 4. In addition, the network server 114 may include a communication protocol layer 2716, which provides low-level communication functions to server communications software. The communication protocol layer 2716 may be, but need not be, the same as the communication protocol layer 2714 of the interface station computer 304.

As shown in Fig. 27, the network server 114 may communicate through the network 2724 with an issuer authority 2718. The issuer authority 2718 may correspond, for example, to any of the advertiser(s) 108, non-financial media issuer(s) 110, or financial media issuer(s) 112 described above in connection with Fig. 1, or may be any entity designated to represent any of the same.

Overall, the networking arrangement illustrated in Fig. 27 allows the Pocket Vault 102 to access the network server 114. It also allows the interface station computer 304 to access restricted portions of the network server 114, such as, for example, user data stored in the database 406, when access is authenticated through communication from the Pocket Vault 102 to the network server 114. Authentication and access to restricted areas of the network server 114 will be further described below.

In order for the Pocket Vault 102 to perform communications functions, as well as other functions described elsewhere herein, the Pocket Vault 102 may be driven by

control software 2708. Fig. 28 is a block diagram illustrating example components of the control software 2708 that may be disposed on the Pocket Vault 102.

As shown, the control software 2708 may include components such as a communications software module 2802, a card loading module 2804, an RFID tag loading module 2805, an internet settings management module 2806, a synchronization module 2808, a statistics module 2810, and a security module 2812. It should be appreciated, of course, that the control software 2708 is not limited to the illustrative modules shown, and that the control software 2708 may comprise fewer modules or additional modules to perform other functions, such as the functionality described above in connection with Figs. 7-12.

The communications software module 2802 may, for example, be responsible for communications with the network server 114 and with the interface station computer 304, in the manner discussed below.

The card loading module 2804 may, for example, be responsible for loading data for new cards or tokens and storing such data in memory, as well as for transferring this data to the network server 114, when appropriate. Examples of how card/token data may be loaded onto the Pocket Vault 102 are discussed below in connection with Fig. 34.

The RFID tag loading module 2805 may, for example, be responsible for loading data for new RFID tags and storing such data in memory, as well as for transferring this data to the network server 114, when appropriate. Examples of how RFID tag data may be loaded onto the Pocket Vault 102 are discussed below in connection with Fig. 40.

Internet settings management module 2806 may, for example, be responsible for managing the storage and use of internet settings by the Pocket Vault 102. Such internet settings may, for example, correspond to any of the internet settings 2722 that may be stored on the interface station computer 304. The internet settings management module 2806 may allow a user to store, manage, and transfer internet settings, e.g., cookies and preference settings, from one computer to another. Operation of the internet settings management module 2708 will be further described below in connection with the steps 3310 and 3320 of the routine 3024 (Fig. 33).

The synchronization module 2808 may, for example, be responsible for synchronizing data and settings stored on the Pocket Vault 102 with data and settings stored on the network server 114. Operation of the synchronization module 2808 is described below in connection with Fig. 35.

The statistics module 2810 may, for example, collect statistics concerning use of the Pocket Vault 102. Such statistics may, for example, include information such as the number of accesses to various cards stored in the memory of the Pocket Vault 102, the number of financial transactions engaged in, the date of the last update of the Pocket Vault 102, the total amount and kind of data transferred between the Pocket Vault 102 and each interface station 104 and/or the network server 114. In addition, the statistics module 2810 may be adapted to be customized by the user.

The security module 2812 may, for example, ensure security of authentication and communications. All communications to and from the network server 114 and the interface station 104 may be encrypted by the security module 2812, so that any attacker who intercepts those communications will receive no useful information.

Any of numerous types of encryption may be used to satisfactorily protect communications between the Pocket Vault 102 and the other devices in the network. For example, one of the asymmetric-key encryption types, such as public key encryption or private key encryption, may be used. These public/private encryption techniques are well known in the art and therefore will not be described here in detail. Alternatively, one-time pad encryption or other encryption techniques may be used to achieve a similar objective.

As discussed above, the Pocket Vault 102 may be adapted to not release any personal or secure information, even encrypted, until the holder presents satisfactory verification of his or her identity, such as, for example, presenting the holder's fingerprint to the fingerprint scanner 220 or entering a password. In addition, fingerprint and password protection may be used together for authentication purposes, such that personal or secure information can be transferred or released only if the holder has been successfully authenticated using both techniques.

In alternative embodiments, security may be implemented using different measures, or may be omitted altogether in situations where the interface station computer 304 is a trusted host. In addition, security module 2812 may be called on to perform security functions in situations other than communicating with the network server 114 and the interface station computer 304.

The manner of communication among the Pocket Vault 102, the network server 114, and an interface station computer 304 will now be described in connection with Figure 29. Figure 29 is a data flow diagram illustrating how data may be transferred

between the Pocket Vault 102 and a user interface 2902 of the interface station computer 304. The user interface 2902 may, for example, comprise a web browser included in the communications software 2710 running on the interface station computer 304. Alternatively, it may be a stand-alone application that allows a user to interact with the communications software 2710 and, through it, interact with a website located on the network server 114.

In the illustrative embodiment shown, the data transfer takes place via the communication driver 2712, the network server 114, and the communications software 2710, data can flow in both directions at all connection points, and all communications between the Pocket Vault 102 and the user interface 2902 of the interface station computer 304 pass through the network server 114.

Using the arrangement shown, the user may, for example, update settings on the Pocket Vault 102 by using the user interface 2902 and the communication software 2710 to update settings on the network server 114, and then instructing the network server 114 to update settings on the Pocket Vault 102 via the communication driver 2712.

In one embodiment, the network server 114 implements a website, where user information may be selectively stored and accessed by a person using the communication software 2710 (e.g., a web browser) running on the interface station computer 304, and any user may access the website on the network server 114. However, the website may have a so-called "restricted area" which can be accessed only after the user has authenticated his or her identity. As used herein, the term "restricted area" or "restricted information" means any data that is not available to general public without some sort of authentication. For example, each user may have preferences stored in the database 406 that would indicate how the main site should be presented to that user. Those preferences will not be available to other users. In addition to such relatively low-security settings, such as website preferences, database 406 may also contain private user information, such as information about a user's credit cards and identity information. Access to this restricted information may be limited, for example, to only "authenticated" users.

Authentication of a Pocket Vault holder may be achieved, for example, by the holder applying a fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, interfacing the Pocket Vault 102 with the interface unit 302 (which acts essentially as a pass-through device), and establishing a connection between the Pocket Vault 102 and

the network server 114 via the communication driver 2712. Based on communications with the Pocket Vault 102 via this "connection," the website may determine: (1) whether the Pocket Vault 102 has been "validated," i.e., whether a fingerprint has been stored in the fingerprint memory of the Pocket Vault 102 and whether validation information (e.g., a PKI certificate) is present on the Pocket Vault 102, and (2) whether the Pocket Vault 102 has been authenticated, i.e., whether the fingerprint recently scanned by the Pocket Vault 102 matched the fingerprint stored in the fingerprint memory of the Pocket Vault 102. If the website determines that the Pocket Vault 102 has not yet been validated, the user may be given an option to validate the Pocket Vault 102 using the website software. If the website determines that the Pocket Vault 102 has been validated and authenticated, then the network server 114 may enable the authenticated holder to access or perform functions relating to some or all of the restricted area of the database 406 containing that holder's information.

Communication driver 2712 may be a light-weight application that can access and modify the internet settings 2722, and can also access communications protocol layer 2714, but cannot transfer information to any other software programs. For example, the communication driver 2712 may access the internet settings 2722 in order to determine that the interface station computer 304 is connected to the network 2724 through a dial-up connection; following that, it may initiate the dial-up connection or use an established connection through the communications protocol layer 2714 in order to tunnel packets from the Pocket Vault 102 to the network 2724.

Fig. 30 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO ACCESS WEBSITE routine 1422 shown in Fig. 14, which may be executed by the controller 308 of the interface station computer 304. As discussed above in connection with Fig. 14, it should be appreciated that this routine need not be accessed as a result of a user selecting it from the menu displayed in the step 1402. Rather, a user may simply use a browser to directly log onto the website on the network server 114.

As shown, the routine 1422 begins at a step 3002, wherein the interface station computer 304 is caused to access the website on the network server 114, e.g., by using a browser to access the website.

After the step 3002, the routine 1422 proceeds to a step 3004, wherein it is determined whether the requisite communication drivers 2712 have been installed.

When, at the step 3004, it is determined that the requisite communication drivers 2712 have not been installed, the routine 1422 proceeds to an INSTALL DRIVER(S) routine 3006 (discussed below in connection with Fig. 31), which is responsible for installing the communication drivers 2712.

After the routine 3006 has completed, the routine 1422 proceeds to a step 3008, wherein the communication drivers 2712 are caused to become operational.

When, at the step 3004, it is determined that the requisite drivers 2712 have already been installed, the routine 1422 proceeds directly to the step 3008 (discussed above).

After the step 3008, the routine 1422 proceeds to steps 3010-3016, wherein attempts are made to establish a connection between the Pocket Vault 102 and the website on the network server 114 within a time out period determined by the step 3014. Each time it is determined that the connection has not yet been established, the user is prompted to interface the Pocket Vault 102 with the interface unit 302 and to connect the interface unit 302 to the interface station computer 304 (e.g., using a USB cable).

When, during the steps 3010-3016, it is determined that a connection has not been established between the Pocket Vault 102 and the website in a timely manner, the routine 1422 proceeds to a step 3026, wherein a message is displayed to the user regarding the unsuccessful communication attempt between the Pocket Vault 102 and the website on the network server 114.

After the step 3026, the routine 1422 terminates.

When, during the steps 3010-3016, it is determined that a connection has been successfully established between the Pocket Vault 102 and the website on the network server 114, the routine 1422 proceeds to a step 3018, wherein it is determined whether the Pocket Vault 102 has been validated, e.g., whether a holder's fingerprints and a PKI certificate are stored therein. The website may, for example, make this determination based upon the messages exchanged during the handshaking protocol engaged in between the Pocket Vault 102 and the network server 114.

When, at the step 3018, it is determined that the Pocket Vault 102 has not yet been validated, the routine 1422 proceeds to a NEW POCKET VAULT HOLDER routine 3020, which is discussed below in connection with Fig. 32.

When, at the step 3018, it is determined that the Pocket Vault 102 has already been validated, the routine 1422 proceeds to an EXISTING POCKET VAULT HOLDER routine 3024, which is discussed below in connection with Fig. 33.

After completion of the EXISTING POCKET VAULT HOLDER routine 3024, the routine 1422 terminates.

After completion of the NEW POCKET VAULT HOLDER routine 3020, the routine 1422 proceeds to a step 3022, wherein it is determined whether a new holder was successfully validated.

When, at the step 3022, it is determined that a new holder was successfully validated, the routine 1422 proceeds to the EXISTING POCKET VAULT HOLDER routine 3024 (discussed above).

When, at the step 3022, it is determined that a new holder was not successfully validated, the routine 1422 terminates.

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine 3006 shown in Fig. 30.

As shown, the routine 3006 begins at a step 3102, wherein the necessary communication drivers 2712 are downloaded from another computer, e.g., a website on the World Wide Web.

After the step 3102, the routine 3006 proceeds to steps 3104-3108, wherein the necessary communication drivers 2712 are installed on the interface station computer 304 and registered with network server 114, and the preferences for the communication drivers 2712 are set either automatically or in response to user input. During the step 3106, the communication driver 2712 may communicate with the network server 114 in order to register itself and its attributes. Among these attributes can be such things as a unique identifier for the interface station computer 304 on which that driver is installed, the identity of the user registering it, and other such items. The preferences that may be set by the user during the step 3108 may, for example, include information such as how and where to access the internet settings 2722, how many attempts at connection should be performed, etc.

After the step 3108, the routine 3006 terminates.

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine 3020 shown in Fig. 30.

As shown, the routine 3020 begins at a step 3202, wherein it is determined whether the new holder has indicated that he or she has already established an account with the website on the network server 114.

When, at the step 3202, it is determined that the new holder has not indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3204, wherein a new account is established on the website on the network server 114 in response to user input to a browser running on the interface station computer 304.

After the step 3204, the routine 3020 proceeds to a step 3206, wherein the new holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 while the Pocket Vault 102 is interfaced with the interface unit 302. The user is further prompted to follow the directions on the Pocket Vault 102. As discussed above in connection with Figs. 7 and 8, when a fingerprint is applied to a fingerprint scanner 220 of an un-validated device, the user is instructed by the Pocket Vault to apply six finger prints (three from one finger on the left hand and three from one finger on the right hand) sequentially to the fingerprint scanner 220, waiting for a beep each time. As discussed in connection with Fig. 8, after the new holder has completed this task, an encrypted message including the Pocket Vault ID may be released from the Pocket Vault to the interface unit 302. Because of the established connection between the Pocket Vault 102 and the website on the network server 114, this encrypted message should reach the website. And, in response to receiving this encrypted message, the website should release encrypted validation information (e.g., a PKI certificate) back to the Pocket Vault 102 via the established connection.

After the step 3206, the routine 3020 proceeds to steps 3208-3210, wherein it is determined whether the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before a timeout period has elapsed.

When, at the step 3210, it is determined that the timeout period elapsed before the encrypted message including the Pocket Vault ID was released to the website, the routine 3020 proceeds to a step 3220, wherein a message is displayed to the user concerning the unsuccessful attempt to validate the Pocket Vault holder.

After the step 3220, the routine 3020 terminates.

When, at the steps 3208-3210, it is determined the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before the timeout period elapsed, the routine 3020 proceeds to a step 3212, wherein it is determined

whether the website has released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102.

When, at the step 3210, it is determined that the timeout period elapsed before the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102, the routine 3020 proceeds to the step 3220 (discussed above).

When, at the step 3210, it is determined that the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102 before the timeout period elapsed, the routine 3020 proceeds to a step 3216, wherein a message is displayed to the user concerning the successful validation of the new Pocket Vault holder.

After the step 3216, the routine 3020 terminates.

When, at the step 3202, it is determined that the new holder has indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3218, wherein a check is made to verify the holder's identity. The holder may, for example, be required to enter personal information, such as name, contact information, and security information to verify his or her identity.

When, at the step 3218, it is determined that the holder has successfully verified his or her identity, the routine 3020 proceeds to the step 3206 (discussed above), with the holder's previously-stored account information being used for the new Pocket Vault 102.

When, at the step 3218, it is determined that the holder has not successfully verified his or her identity, the routine 3020 proceeds to the step 3220 (discussed above).

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine 3024 shown in Fig. 30.

As shown, the routine 3024 begins at a step 3302, wherein it is determined whether the Pocket Vault 102 has been authenticated, e.g., whether the Pocket Vault 102 has determined that a fingerprint applied to the fingerprint scanner 220 matches one of the fingerprints stored in the fingerprint memory of the Pocket Vault 102. This authentication procedure may operate as described above in connection with the step 712 (Fig. 7), or an additional or different routine may be employed (e.g., as part of the security module 2812 described above in connection with Fig. 28) to determine whether the holder has successfully authenticated his or her identity, thereby enabling the network server 114 to establish a "trust" relationship with the Pocket Vault 102.

When, at the step 3302, it is determined that the Pocket Vault 102 has not been properly authenticated, the routine 3024 proceeds to a step 3304, wherein the holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102 while the Pocket Vault 102 is interfaced with the interface unit 302, i.e., while keeping the connection established between the Pocket Vault 102 and the website on the network server 114.

As shown, the step 3306 determines whether the Pocket Vault 102 has been properly authenticated prior to the expiration of a timeout period.

When, at the step 3306, it is determined that the timeout period elapsed before the Pocket Vault 102 was authenticated, the routine 3024 proceeds to a step 3308, wherein a message is displayed indicating that the authentication attempt was unsuccessful.

After the step 3308, the routine 3024 terminates.

When, at the step 3302, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 3024 proceeds to a step 3310, wherein the communication driver 2712 causes the internet settings 2722 of the interface station computer 304 to be adjusted to reflect certain internet settings stored in the Pocket Vault 102, e.g., by the internet settings management module 2806. In this manner, the internet settings of the Pocket Vault 102 may be "ported" to the interface station computer 304 so that the browser operating on the interface station computer 304 may take advantage of those settings while the Pocket Vault 102 is connected to the website on the network server 114 via the communication driver 2712. The internet settings of the Pocket Vault 102 that may be ported to the interface station computer 304 in this manner may comprise, for example, the network name and identification of the Pocket Vault 102, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The internet settings on the Pocket Vault 102, and porting of the same to the interface station computer 304, may be managed, for example, by one or more modules of the control software, e.g., the internet settings management module 2806. In one embodiment, the user may elect which internet settings are to be ported to the interface

station computer 304 during the step 3310. This functionality may be accomplished, for example, during a SET PREFERENCES routine 3324 (described below in connection with Fig. 39).

After the step 3310, the routine 3024 proceeds to a step 3312, wherein it is determined whether one of several "functions" has been selected. In the illustrative embodiment shown, the seven available functions are: (1) CARD LOADING (see CARD LOADING routine 3314 -- discussed below in connection with Fig. 34), (2) RFID TAG LOADING routine 3315 – discussed below in connection with Fig. 40, (3) SYNCHRONIZATION (see SYNCHRONIZATION routine 3316 -- discussed below in connection with Fig. 35), (4) RECOVERY (see RECOVERY routine 3318 -- discussed below in connection with Fig. 36), (5) IDENTITY PORTING OPTIONS (see IDENTITY PORTING OPTIONS routine 3320 -- discussed below in connection with Fig. 337), (6) BACKUP (see BACKUP routine 3322 -- discussed below in connection with Fig. 38), (7) SET PREFERENCES (see SET PREFERENCES routine 3324 -- discussed below in connection with Fig. 39), AND (8) TERMINATE SESSION (see step 3326). It should be appreciated that the invention is not limited to the specific functions shown, and that additional, different or fewer functions may be employed.

It should further be appreciated that some or all of the illustrated functions, or operations relating to such functions, may be initiated automatically or may require user initiation, depending on the setting of preferences. For example, the SYNCHRONIZATION routine 3316 may be initiated automatically after completion of the step 3310, if preferences so indicate. Alternatively, certain steps required to accomplish synchronization of the Pocket Vault 102 and the website on the network server 114 may be taken, without actually completing the synchronization. For example, the synchronization module 2808 of the control software 2708 may automatically initiate a comparison of the contents of the Pocket Vault 102 and the website to determine what data should be transferred if synchronization is initiated. Software on the network server 114 may also or alternatively perform a similar comparison function automatically, if so desired.

Moreover, it should be understood that, in some embodiments, some of the above-noted functions may be performed without first requiring a Pocket Vault 102 to be authenticated. For example, some functions may involve the transfer of public or non-

sensitive data, and may not require protection via the authentication verification step 3302.

As shown in Fig. 33, when any of the above-listed seven functions is selected, either automatically or in response to user input, the selected function is performed. For each of functions 3314, 3316, 3318, 3320, 3322, and 3324, after performing the routine associated with the function, the routine 3024 proceeds to a step 3332, wherein it is determined whether the connection between the Pocket Vault 102 and the website on the network server 114 is still established.

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is still established, the routine 3024 returns to the step 3312 (discussed above).

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is no longer established, the routine 3024 proceeds to a step 3327, wherein some or all of the internet settings 2722 are ported from the interface station computer 304 to the Pocket Vault 102. The communication driver 3712 may cause the settings to be ported directly to the Pocket Vault 102 from the interface station computer 304 (via the interface unit 302), or the settings may be transferred first to the network server 114 and then to the Pocket Vault 102 (via the connection between the network server 114 and the Pocket Vault 102). In some embodiments, only certain types or classes of settings, e.g., certain type of cookies, PKI certificates, etc., are ported from the interface station computer 304 to the Pocket Vault 102 in this manner. The classes or types of settings that are ported during the step 3327 may, for example, be determined by the user in some embodiments. For example, the user may set certain preferences, e.g., during the SET PREFERENCES routine 3324 or by manipulating the Pocket Vault 102 directly, that control the nature and type of internet settings that are ported to the Pocket Vault 102 from the interface station computer 304 during the step 3327.

After the step 3327, the routine 3024 proceeds to a step 3328, wherein the communication driver 2712 causes the internet settings 2722 on the interface station computer 304 to return to their original state, i.e., the configuration the internet settings 2712 were in before they were altered in the step 3310.

After the step 3328, the routine 3024 proceeds to a step 3330, wherein any cached web pages or other information temporarily stored in the interface station computer 304

during the communication session between the Pocket Vault 102 and the website on the network server 114 are deleted from cache and other memory in the interface station computer 304. Thus, after completion of the step 3330, the interface station computer 304 is in essentially the same state it was in prior to the beginning of the routine 1422. The communication driver 2712 may remain on the interface station computer 304 or may be deleted in connection with the step 3330. If the communication driver 2712 is kept on the interface station computer 304, any cache or other memory associated with it that might store personal or sensitive information may also be erased. In some embodiments, the communication driver 2712 caches or stores very little, if any, information that is passed between the Pocket Vault 102 and the website on the network server 114. In any event, the communication driver 2712 may be constructed such that no useful data, i.e., data that reflects any personal or sensitive information, remains on it after completion of the step 3330.

When, at the step 3312, the holder chooses the TERMINATE SESSION function, the connection between the Pocket Vault 102 and the website on the network server 114 is de-established, and the routine 3024 proceeds immediately to the steps 3327, 3328 and 3330 (discussed above).

After the step 3330, the routine 3024 terminates.

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine 3314 shown in Fig. 33.

As shown, the routine 3314 begins at a step 3402, wherein a determination is made as to whether the card desired to be loaded is "swipeable." The user may, for example, be prompted to indicate whether the card has an operational magnetic stripe disposed thereon.

When, at the step 3402, the user indicates that the card does not have an operational magnetic stripe, the routine 3314 proceeds to a step 3406, wherein the user is prompted (e.g., via the browser on the interface station computer 304) to input information to be used in creating a card account.

When, at the step 3402, the user indicates that the card does have an operational magnetic stripe, the routine 3314 proceeds to the step 3410, wherein the user is prompted to swipe the card through the stripe reader 315 of the interface unit 302.

After the step 3406, the routine 3314 proceeds to steps 3408 and 3409, wherein it is determined whether the interface station computer 304 has received the information

from a card swiped through the stripe reader 315 of the interface unit 302 prior to the expiration of a timeout period.

When, at the step 3409, it is determined that the timeout period elapsed before information from a swiped card was received, the routine 3314 proceeds to a step 3411, wherein a message is displayed to the user concerning the failure to properly read the magnetic stripe.

After the step 3411, the routine 3314 returns to the step 3402 (discussed above). Thus, when a user is unsuccessful in swiping a card one or more times, the user may determine that the magnetic stripe is non-operational, and may indicate at the step 3402 that the card is not swipeable. The user may thereafter create an account for the card manually at the step 3410 (discussed above).

After the step 3410, the routine proceeds to a step 3412, wherein the website on the network server 114 determines whether the account for the card is valid. This determination may be made, for example, by confirming that the card is owned by the person attempting to add it to his or her Pocket Vault 102, that the card has not expired, etc.

When, at the step 3408, it is determined that information from the swiped card has been received prior to the expiration of the timeout period, the routine 3314 proceeds to the step 3412 (discussed above), wherein a determination is made as the validity of the account based upon the information read by the stripe reader 315.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is not valid, the routine 3314 proceeds to a step 3414 wherein appropriate security precautions are taken.

After the step 3414, the routine 3314 terminates.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is valid, the routine 3314 proceeds to a step 3416, wherein the information for the card is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3416, the routine 3314 proceeds to a step 3418, wherein a message is displayed that indicates the card has been successfully loaded onto the Pocket Vault 102 for use in future transactions.

After the step 3418, the routine 3314 terminates.

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine 3316 shown in Fig. 33.

As shown, the routine 3316 begins at a step 3502, wherein certain parameters required to synchronize the Pocket Vault 102 to the website on the network server 114 are determined based upon user preferences and the ID of the Pocket Vault 102. For example, if a holder has two or more Pocket Vaults 102, the holder may wish to elect one of them to be a master for synchronization purposes, or the holder may even elect to have the website act as the master. When a holder has more than one Pocket Vault 102, the holder also may desire to be prompted to select either the current date or the date of the last synchronization as the basis for the synchronization operation.

After the step 3502, the routine 3316 proceeds to a step 3504, wherein the website on the network server 114 generates sets of current data to transfer to the Pocket Vault 102. The website may, for example, compare its current data to the data stored on the Pocket Vault 102 so as to identify any data it needs to receive from the Pocket Vault 102 to properly synchronize therewith.

After the step 3504, the routine 3316 proceeds to steps 3506 and 3508, wherein it is determined whether the Pocket Vault 102 has indicated that it is ready to synchronize prior the expiration of a timeout period (measured by the step 3508). The Pocket Vault 102 may, for example, also be performing a similar comparison (e.g., using the synchronization module 2808) between its data and the data stored on the website of the network server to determine what data it needs to receive from the website to properly synchronize therewith.

When at the step 3508, it is determined that the timeout period has elapsed before the Pocket Vault 102 had indicated its readiness to synchronize, the routine 3316 proceeds to a step 3510, wherein a message is generated indicating the attempt to synchronize the Pocket Vault 102 with the website on the network server 114 has failed.

After the step 3510, the routine 3316 terminates.

When at the step 3506, it is determined that the Pocket Vault 102 has indicated its readiness to synchronize with the website prior to the expiration of the timeout period, the routine 3316 proceeds to a step 3512, wherein accumulated synchronization data is transferred from the website to the Pocket Vault 102, and vice versa, via the communication driver 2712.

After the step 3512, the routine 3316 proceeds to a step 3516, wherein the date of the successful synchronization is stored in both the Pocket Vault 102 and the network server 114.

After the step 3516, the routine 3316 proceeds to a step 3518, wherein a message is generated indicating that the Pocket Vault 102 has been successfully synchronized with the website on the network server 114.

After the step 3518, the routine 3316 terminates.

Figure 36 is a flow diagram illustrating an example implementation of the RECOVERY routine 3318 shown in Fig. 33.

As shown, the routine 3318 begins at a step 3602, wherein the website on the network server 114 compiles all data necessary to recover the Pocket Vault 102 to its state as of the last time its contents were synchronized with the website of the network server 114 (e.g., using the routine 3316 – described above) or backed up on the website of the network server 114 (e.g., using routine 3322 – described below).

After the step 3602, the routine 3318 proceeds to step 3604, wherein the data compile in the step 3602 is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712, and a determination is made as to where that downloading has completed prior to the expiration of a timeout period measured at the step 3606.

When, at the step 3606, it is determined that the timeout period elapsed prior to the downloading being completed, the routine 3318 proceeds to a step 3608, wherein a message is generated indicating that the attempted recovery was unsuccessful.

After the step 3606, the routine 3318 terminates.

When, at the step 3606, it is determined that the downloading was completed in a timely manner, the routine 3318 proceeds to a step 3610, wherein a message is generated indicating that the attempted recovery of data to the Pocket Vault 102 was successful.

After the step 3610, the routine 3318 terminates.

Figure 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine 3320 shown in Fig. 33.

As shown, the routine 3320 begins at a step 3702, wherein the internet settings 2722 from the interface station computer 304 are downloaded from the interface station computer 304 to the website on the network server 114.

After the step 3702, the routine 3320 proceeds to a step 3704, wherein the website on the network server 114 compiles and displays the downloaded internet settings to the user via the browser on the interface station computer 304. The settings may be displayed to the user in any of a number of ways. Preferably, the settings are displayed in a manner that enables the user to readily distinguish between various classes of settings, and that permits the user to readily identify the purpose of each type of setting. In some embodiments, only a subset of the all of the internet settings 2722 (e.g., only settings such as cookies and PKI certificates) are transferred to the website for possible modification by the user.

After the step 3704, the routine 3320 proceeds to steps 3706 and 3708, wherein the user is given an opportunity to modify the displayed internet settings. The user may, for example, elect to keep certain cookies that were retained among the internet settings 2722, while choosing to discard others.

When at the step 3708, the user has indicated that he or she has completed any modifications of the retrieved internet settings 2722, the routine 3320 proceeds to a step 3710, wherein the modified internet settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3710, the routine 3320 terminates.

When at the step 3706, it is determined that the user did not elect to modify any settings, the routine 3320 terminates.

Figure 38 is a flow diagram illustrating an example implementation of the BACKUP routine 3322 shown in Fig. 33.

As shown, the routine 3322 begins at a step 3802, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, asking the Pocket Vault 102 to send the website backup data. This backup data may, for example, constitute all data necessary to place the Pocket Vault 102 back into its present state if any portion of data on the Pocket Vault 102 was lost, or to place a new Pocket Vault 102 into the same state as the backed up Pocket Vault 102 (e.g., using the RECOVERY routine 3318 – discussed above).

After the step 3802, the routine 3322 proceeds to steps 3804 -3806, wherein it is determined whether the requested backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 before the expiration of a timeout period (measured by the step 3806).

When, at the step 3806, it is determined that the timeout period elapsed prior to the backup data being successfully transferred, the routine 3322 proceeds to a step 3808, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that a communication error has occurred and that the backup operation was unsuccessful.

After the step 3808, the routine 3322 terminates.

When, at the step 3804, the routine 3322 determined that, before the timeout period, the backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712, the routine 3322 proceeds to a step 3810, wherein the received backup data is stored by the network server 114, e.g., for use in connection with the RECOVERY routine 3318.

After the step 3310, the routine 3322 proceeds to a step 3812, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the backup operation was successfully completed.

After the step 3312, the routine 3322 terminates.

Figure 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine 3324 shown in Fig. 33. The SET PREFERENCES routine 3324 permits the holder to set or alter preferences on his or her Pocket Vault 102 using a browser on the interface station computer 104.

As shown, the routine 3324 begins at a step 3902, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, requesting the Pocket Vault 102 to transmit all "preferences" information stored on the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712. This information may, for example, comprise definitions of home pages, connection of secure and non-secure media, order of media presentment, sort orders, user interface options, synchronization defaults, etc.

After the step 3902, the routine 3324 proceeds to steps 3904 and 3906, wherein it is determined whether the preferences information has been received from the Pocket Vault 102 prior to the expiration of a timeout period (measured by the step 3906).

When, at the step 3906, it is determined that the timeout period elapsed before the preferences information was transferred from the Pocket Vault 102 to the website, the routine 3324 proceeds to a step 3908, wherein a message is displayed (e.g., on the browser) indicating that a communication error has occurred.

After the step 3908, the routine 3324 terminates.

When, at the step 3904, it is determined that the preferences information has been successfully transferred from the Pocket Vault 102 to the website on the network server 114, the routine 3324 proceeds to a step 3910, wherein the website compiles and displays the current preference settings for the Pocket Vault 102 (e.g., on the browser) in a user friendly manner.

After the step 3910, the routine 3324 proceeds to steps 3912 and 3914, wherein the user is given an opportunity to modify the displayed preference settings.

When, at the step 3912, the user opts not to modify any of the displayed settings, the routine 3324 terminates.

When, at the steps 3912 and 3914, the user opts to modify the displayed settings and indicates that he or she has completed modification thereof, the routine 3324 proceeds to a step 3916, wherein the modified preference settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3918, a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the preference settings for the Pocket Vault 102 were successfully modified.

After the step 3918, the routine 3324 terminates.

Fig. 40 is a flow diagram illustrating an example implementation of the RFID TAG LOADING routine 3315 shown in Fig. 33.

As shown, the routine 3315 begins at a step 4002, wherein the user may use the website on the network server 114 to create an account for the RFID tag to be loaded onto the Pocket Vault 102.

After the step 4002, the routine proceeds to a step 4004, wherein the website on the network server 114 determines whether the account for the RFID tag is valid, for example, by checking with the media that issued the RFID tag account.

When, at the step 4004, it is determined that the account for the RFID tag is not valid, the routine 3315 proceeds to a step 4010, wherein appropriate security precautions are taken.

After the step 4010, the routine 3315 terminates.

When, at the step 4004, a determination is made that the account for the RFID tag is valid, the routine 3315 proceeds to a step 4006, wherein the information for the RFID

tag is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 4006, the routine 3315 proceeds to a step 4008, wherein a message is displayed that indicates the RFID tag information has been successfully loaded onto the Pocket Vault 102 for use in future transactions.

After the step 4008, the routine 3315 terminates.

One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time-sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who make room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room.

After the time period of the guest's room reservation has expired, the Pocket Vault 102 may automatically delete the room key icon. This deletion may occur for the convenience of the Pocket Vault holder, not necessarily for hotel security reasons, since the room's lock will reject any previously-used key card (Chameleon or traditional key card) after the key card's specified time period has expired.

Having thus described at least one illustrative embodiment of the invention, various alterations, modifications and improvements will readily occur to those skilled in the art. Such alterations, modifications and improvements are intended to be within the

spirit and scope of the invention. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention is limited only as defined in the following claims and the equivalents thereto.

What is claimed is:

CLAIMS

1. An apparatus, comprising:

a user authenticator that authenticates an identity of a user; and

a transponder that is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user.

2. The apparatus of claim 1, wherein the wireless signal representing the information and the wireless interrogation signal are radio frequency signals.

3. The apparatus of claim 1 or 2, wherein the apparatus further comprises a memory that stores at least first and second distinct codes, and a user input that permits the user to select any one of the at least first and second codes for transmission in response to an interrogation signal; and wherein the transponder is permitted to emit a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

4. The apparatus of claim 3, further comprising a display that identifies the one of the at least first and second codes the user has selected.

5. The apparatus of claim 3 or 4, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

6. The apparatus of any one of claims 1-5, in combination with an interrogator that wirelessly emits the interrogation signal, and receives from the apparatus the wireless signal representing the information.

7. An apparatus, comprising:

a memory that stores at least first and second distinct codes;

a user input that permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal; and

a transponder that emits a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

8. The apparatus of claim 7, wherein the wireless signal representing the identification information and the wireless interrogation signal are radio frequency signals.

9. The apparatus of claim 7 or 8, further comprising a display that identifies the one of the at least first and second codes the user has selected.

10. The apparatus of any one of claims 7-9, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

11. The apparatus of any one of claims 7-10, in combination with an interrogator that wirelessly emits the interrogation signal, and receives from the apparatus the wireless signal representing the selected one of the at least first and second codes.

12. A token that may be used to engage in a transaction at a point of sale, comprising:

a substrate;

a rewriteable memory, supported by the substrate, that can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale, the substrate and memory being configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory; and

a reconfigurable display, supported by the substrate, that displays at least some of the information that is stored in the rewritable memory.

13. The token of claim 12, wherein rewritable memory stores both an account identifier and a security code separate from the account identifier, and the reconfigurable display displays both the account identifier and the security code.

14. The token of claim 12 or 13, wherein the substrate is substantially the size of a credit card.

15. The token of any one of claims 12-14, wherein the rewritable memory comprises means for selectively storing information on the token that identifies an account that is to be used to engage in the transaction at the point of sale.

16. The token of any one of claims 12-15, wherein the rewritable memory comprises a rewriteable magnetic stripe.

17. The token of any one of claims 12-15, wherein the rewritable memory comprises a circuit that simulates a magnetic stripe.

18. The token of any one of claims 12-15, wherein the rewritable memory comprises a circuit that simulates an account number storage mechanism of a Smartcard.

19. The token of any one of claims 12-18, wherein the reconfigurable display comprises a liquid crystal display (LCD).

20. The token of claim 19, wherein the LCD is flexible.

21. The token of any one of claims 12-29, in combination with an apparatus to which the token is releasably attached, the apparatus being configured to cause the rewritable memory of the token to store the information and to cause the display of the token to display at least some of the information after the token is detached from the apparatus.

22. The combination of claim 21, wherein the rewritable memory comprises means for selectively storing information on the token that identifies an account that is to be used to engage in the transaction at the point of sale.

23. The combination of claim 21 or 22, wherein the apparatus to which the token is releasably attached comprises a memory that stores at least first information identifying a first account and second information identifying a second account, and a user input that permits the user to select one of the first information and second information for use in the transaction, and wherein the apparatus is further configured to cause the rewritable memory of the token to store the selected one of the first information and second information and to cause the display of the token to display at least some of the selected one of the first information and second information.

24. The combination of claim 23, further comprising a display that identifies the one of the first information and second information the user has selected.

25. The combination of claim 23 or 24, wherein the first information and second information correspond to accounts the user holds with respective first and second unrelated media issuers.

26. A method for using an apparatus, comprising steps of:

using the apparatus to authenticate an identity of a user of the apparatus; and

after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal.

27. The method of claim 26, wherein the wireless signal representing the information and the wireless interrogation signal are radio frequency signals.

28. The method of claim 26 or 27, wherein the method further comprises steps of:

manipulating a user input on the apparatus to select one of at least first and second codes stored in memory; and

permitting the transponder to emit a wireless signal representing the selected one of the first and second codes in response to the interrogation signal.

29. The method of claim 28, wherein the method further comprises steps of:

manipulating the user input on the apparatus to select the other of the first and second codes stored in memory; and

permitting the transponder to emit a wireless signal representing the other of the first and second codes in response to the interrogation signal.

30. The method of claim 28 or 29, further comprising a step of:

in response to the user manipulating the user input, displaying to the user an identification of the one of the first and second codes the user has selected.

31. The method of any one of claims 28-30, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

32. The method of any one of claims 26-31, further comprising steps of:

wirelessly emitting an interrogation signal from an interrogator;

receiving the interrogation signal at the transponder;

in response to receiving the interrogation signal, emitting from the transponder a wireless signal representing the information; and

receiving at the interrogator the wireless signal representing the information.

33. The method of claim 32, further comprising a step of authorizing a transaction based upon the information received at the interrogator.

34. A method for using an apparatus, comprising steps of:

manipulating a user input on the apparatus to select one of at least first and second codes stored in memory; and

permitting a transponder of the apparatus to emit a wireless signal representing the selected one of the at least first and second codes in response to a wireless interrogation signal.

35. The method of claim 34, wherein the wireless signal representing the selected one of the at least first and second codes and the wireless interrogation signal are radio frequency signals.

36. The method of claim 34 or 35, wherein the method further comprises steps of:

manipulating the user input on the apparatus to select another of the at least first and second codes stored in memory; and

permitting the transponder to emit a wireless signal representing the other of the at least first and second codes in response to the wireless interrogation signal.

37. The method of any one of claims 34-36, further comprising a step of:

in response to the user manipulating the user input, displaying to the user an identification of the one of the at least first and second codes the user has selected.

38. The method of any one of claims 34-37, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

39. The method of any one of claims 34-38, further comprising steps of:

wirelessly emitting an interrogation signal from an interrogator;

receiving the interrogation signal at the transponder;

in response to receiving the interrogation signal, emitting from the transponder a wireless signal representing the selected one of the at least first and second codes; and

receiving at the interrogator the wireless signal representing the selected one of the at least first and second codes.

40. The method of claim 39, further comprising a step of authorizing a transaction based upon the selected one of the at least first and second codes received at the interrogator.

41. A method for configuring a token to be used to engage in a transaction at a point of sale, comprising steps of:

configuring a rewritable memory of the token to store information that identifies an account that may be used to engage in the transaction at the point of sale, the memory being configured and arranged on the token such that the token can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory; and

configuring a display on the token to display at least some of the information that is stored in the rewritable memory.

42. The method of claim 41, wherein the step of configuring the rewritable memory includes a step of configuring the rewritable memory to store both an account identifier and a security code separate from the account identifier, and the step of configuring the display includes configuring the display to display both the account identifier and the security code.

43. The method of claim 41 or 42, wherein the token is substantially the size of a credit card.

44. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes using a magnetic head to configure a rewriteable magnetic stripe on the token.

45. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes configuring the rewritable memory to cause a simulated magnetic stripe to be generated on the token.

46. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes configuring the rewritable memory to simulate an account number storage mechanism of a Smartcard.

47. The method of any one of claims 41-46, wherein:

the method further comprises a step of manipulating a user input to select one of at least first information identifying a first account and second information identifying a second account;

the step of configuring the rewritable memory includes configuring the rewritable memory to store the selected one of the at least first information and second information; and

the step of configuring the display includes configuring the display to display at least some of the selected one of the at least first information and second information.

48. The method of claim 47, further comprising a step of displaying to the user an identification of the one of the at least first information and second information the user has selected.

49. The method of claim 47 or 48, wherein the first information and second information correspond to accounts the user holds with respective first and second unrelated media issuers.

50. The method of any one of claims 41-49, further comprising steps of:

interfacing the token with an apparatus at the point of sale to permit the apparatus to read the contents of the memory;

displaying the information read from the memory on a display of the apparatus; and

comparing the information displayed on the display of the token with the information displayed on the display of the apparatus to verify the authenticity of the token.

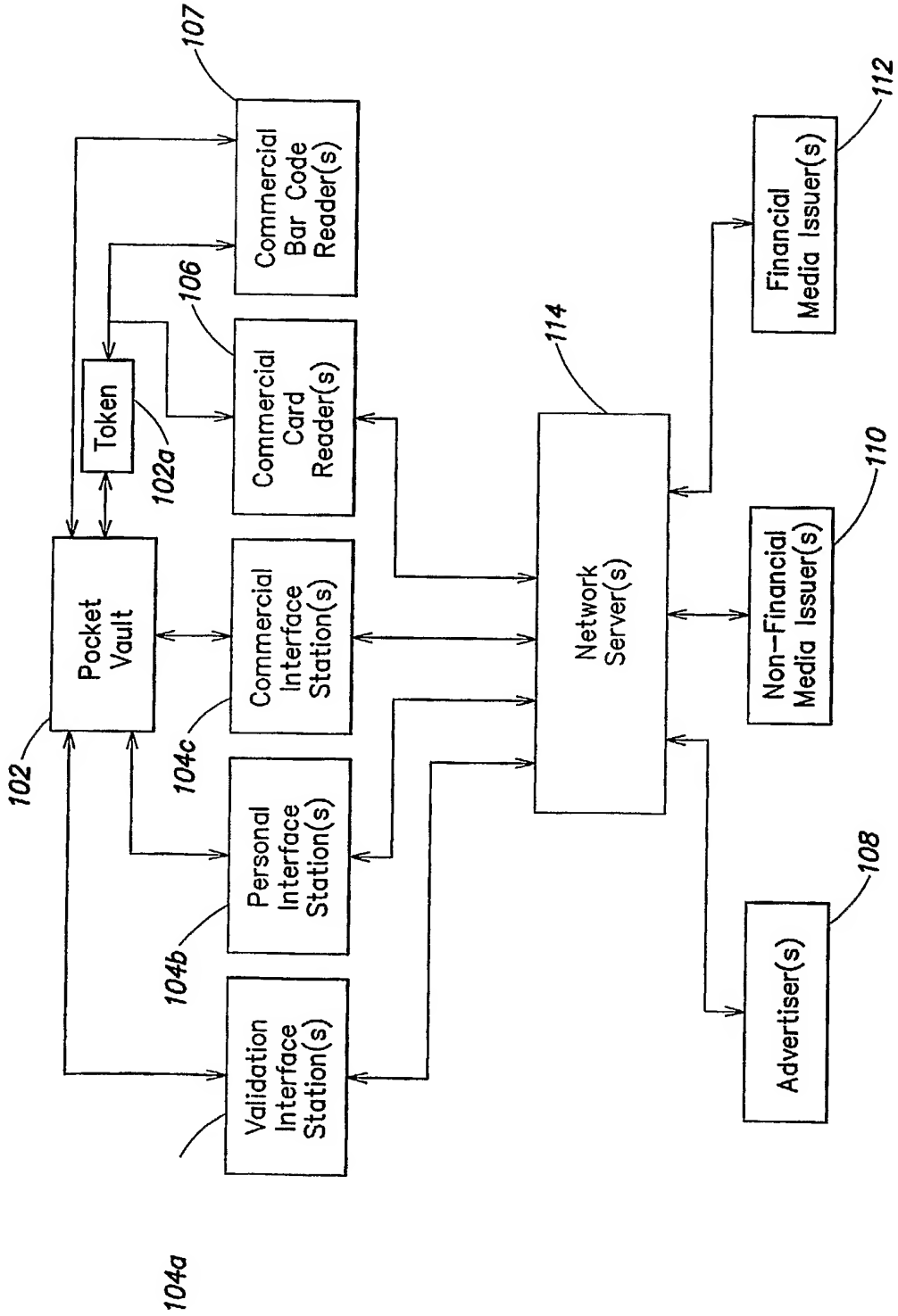

Pocket Vault
102
Token
102a
Commercial Interface Station(s)
104c
Personal Interface Station(s)
104b
Validation Interface Station(s)
104a
Commercial Card Reader(s)
106
Commercial Bar Code Reader(s)
107
Network Server(s)
114
Financial Media Issuer(s)
112
Non-Financial Media Issuer(s)
110
Advertiser(s)
108

FIG. 1

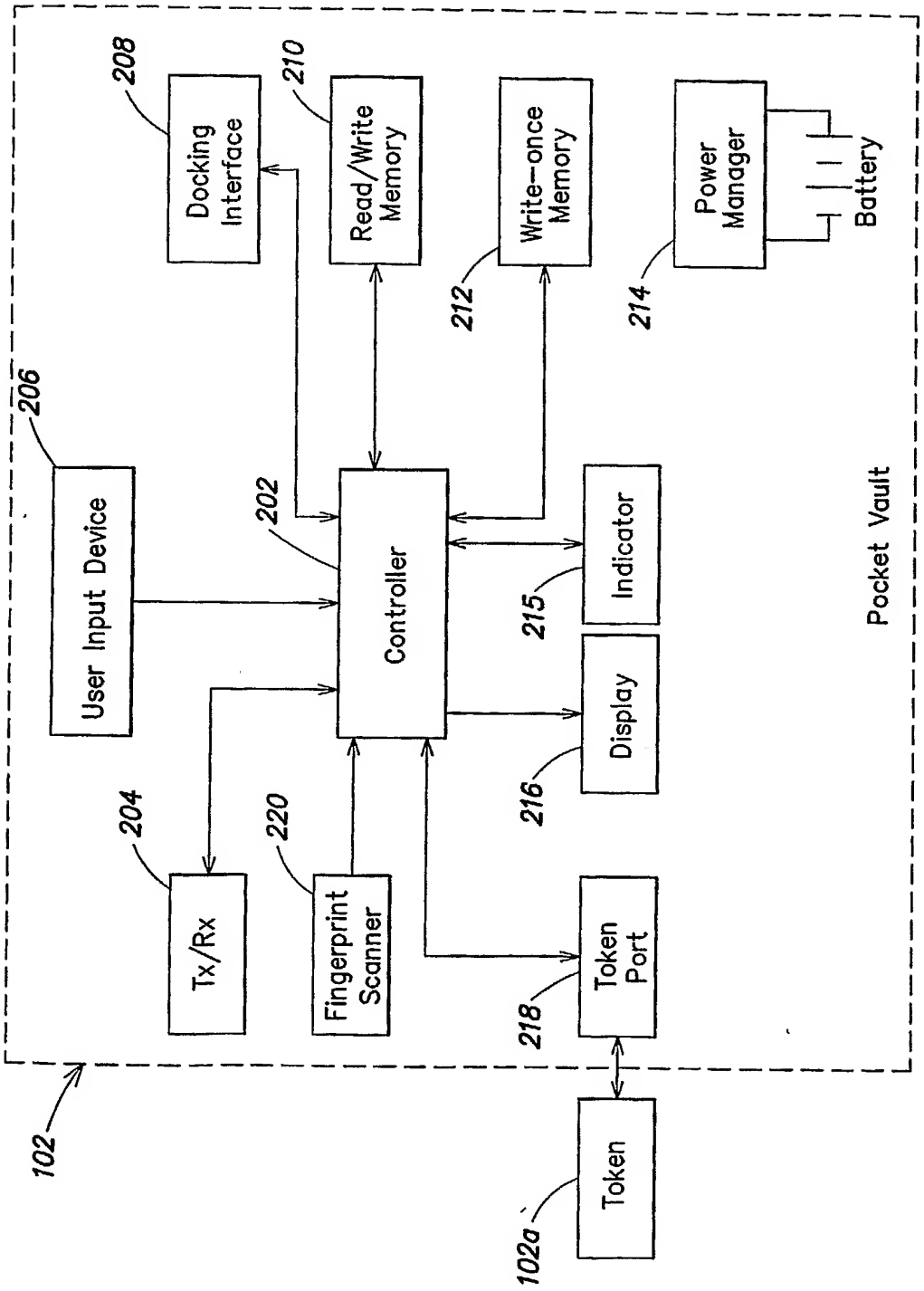

208
Docking Interface
210
Read/Write Memory
Write-once Memory
212
Power Manager
214
Battery
206
User Input Device
202
Controller
Indicator
215
Display
216
Pocket Vault
204
Tx/Rx
220
Fingerprint Scanner
Token Port
218
102
Token
102a

FIG. 2

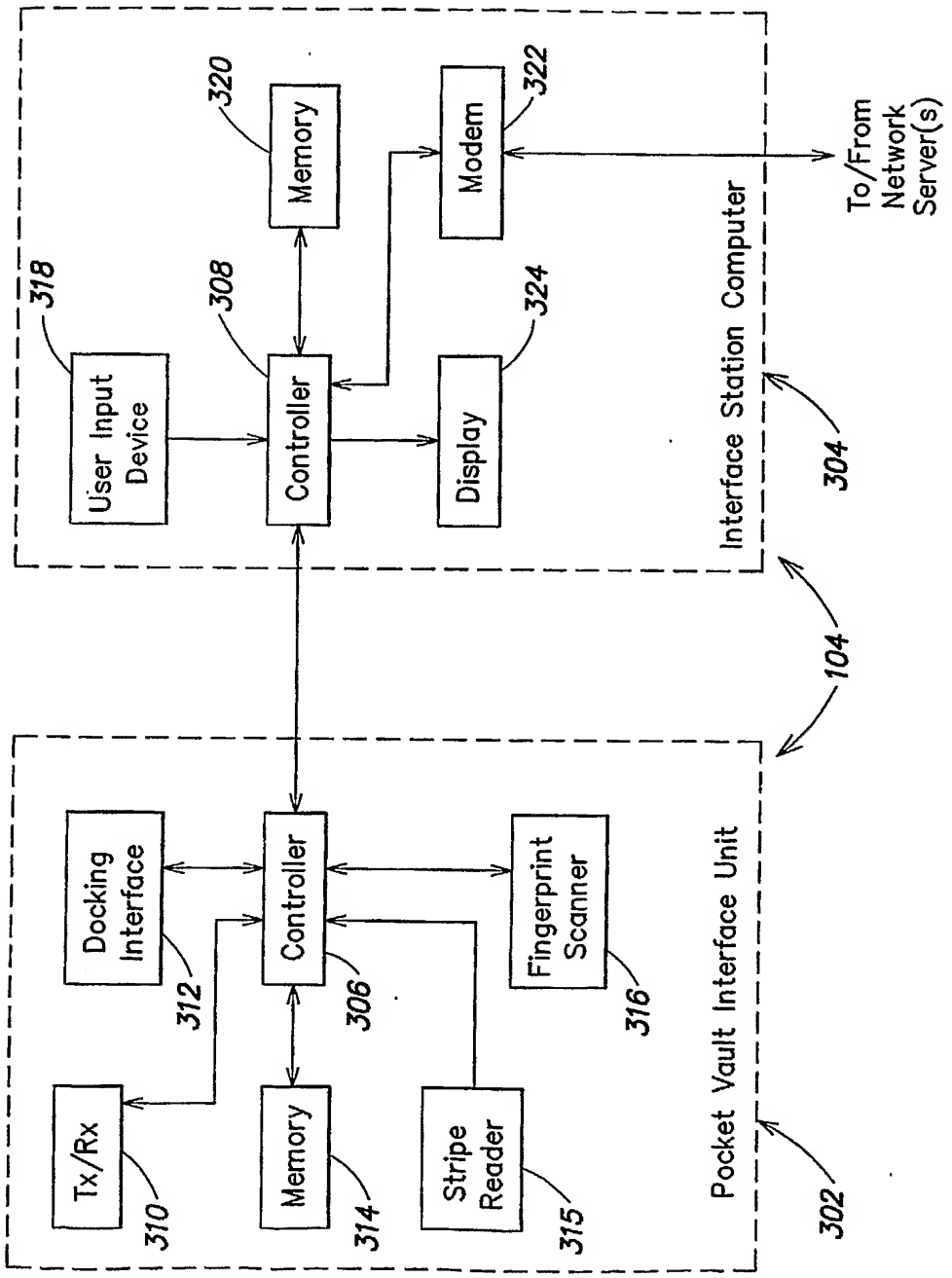

Interface Station Computer
304
User Input Device
318
Controller
308
Memory
320
Modem
322
Display
324
To/From Network Server(s)
104
Pocket Vault Interface Unit
302
Docking Interface
312
Controller
306
Fingerprint Scanner
316
Tx/Rx
310
Memory
314
Stripe Reader
315

FIG. 3

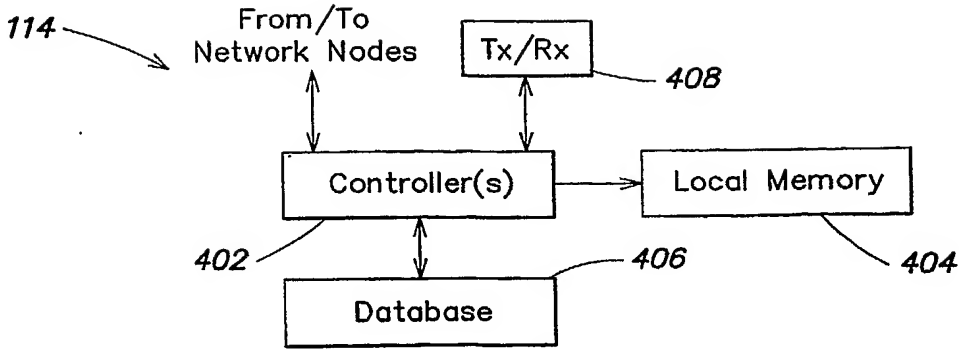


FIG. 4

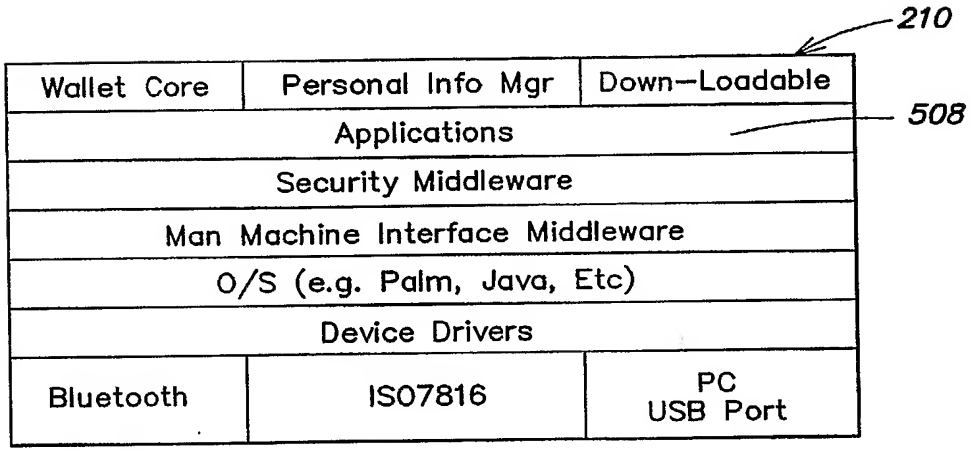


FIG. 5

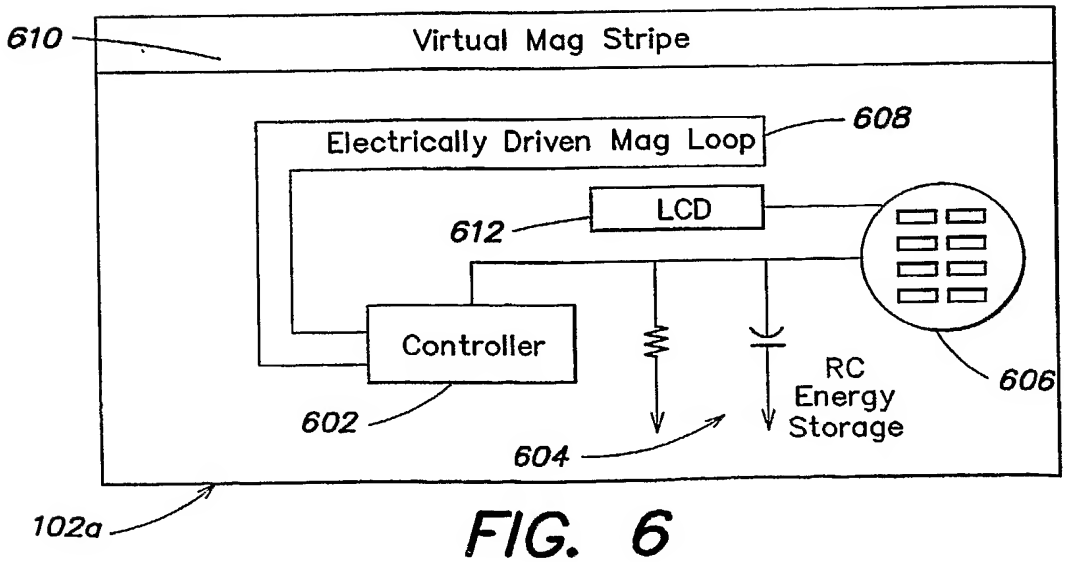


FIG. 6

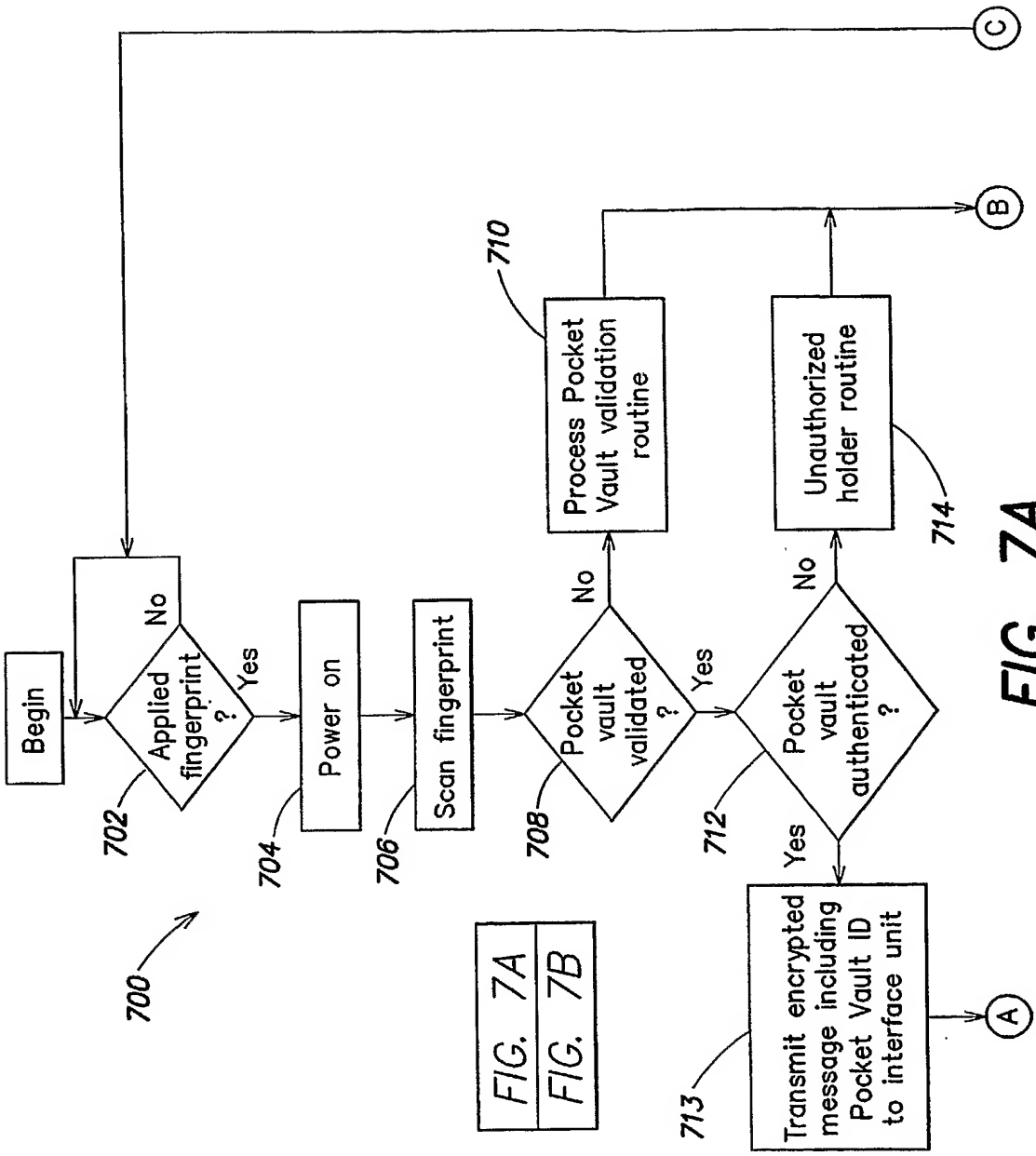


FIG. 7A

FIG. 7A
FIG. 7B

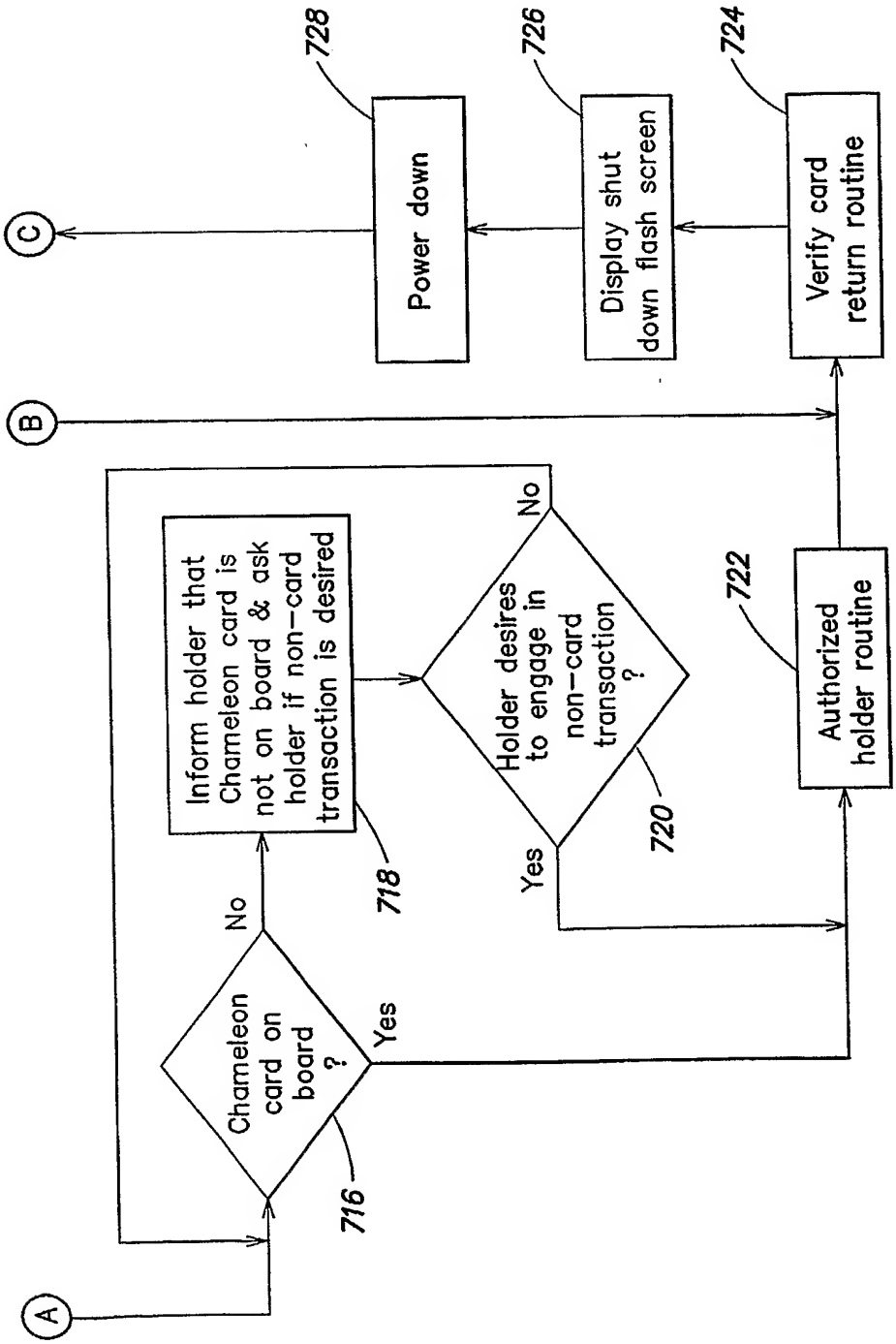

A
B
C
Chameleon card on board ?
716
No
Yes
Inform holder that Chameleon card is not on board & ask holder if non-card transaction is desired
718
Holder desires to engage in non-card transaction ?
720
No
Yes
Authorized holder routine
722
Verify card return routine
724
Display shut down flash screen
726
Power down
728

FIG. 7B

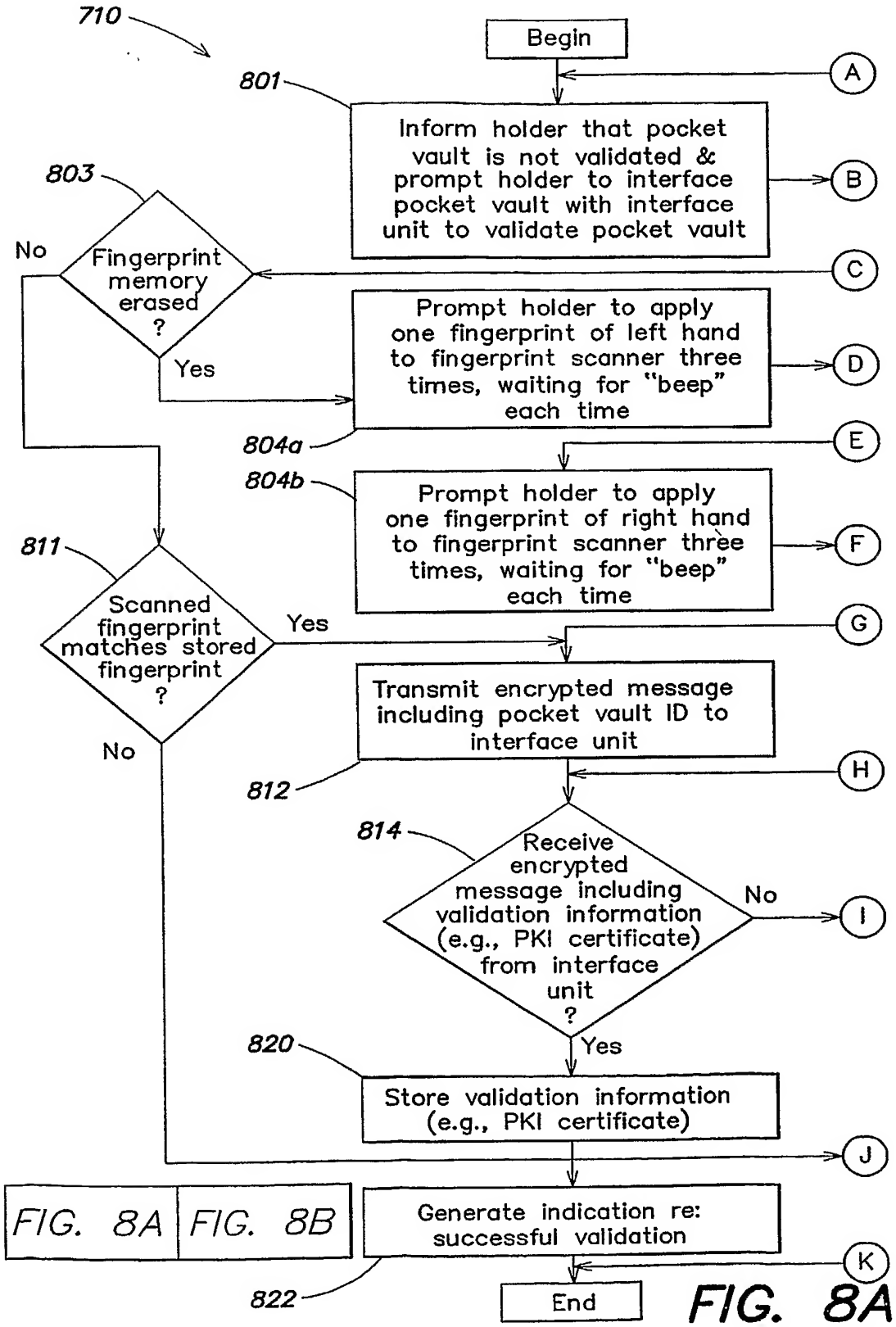


FIG. 8A | FIG. 8B

FIG. 8A

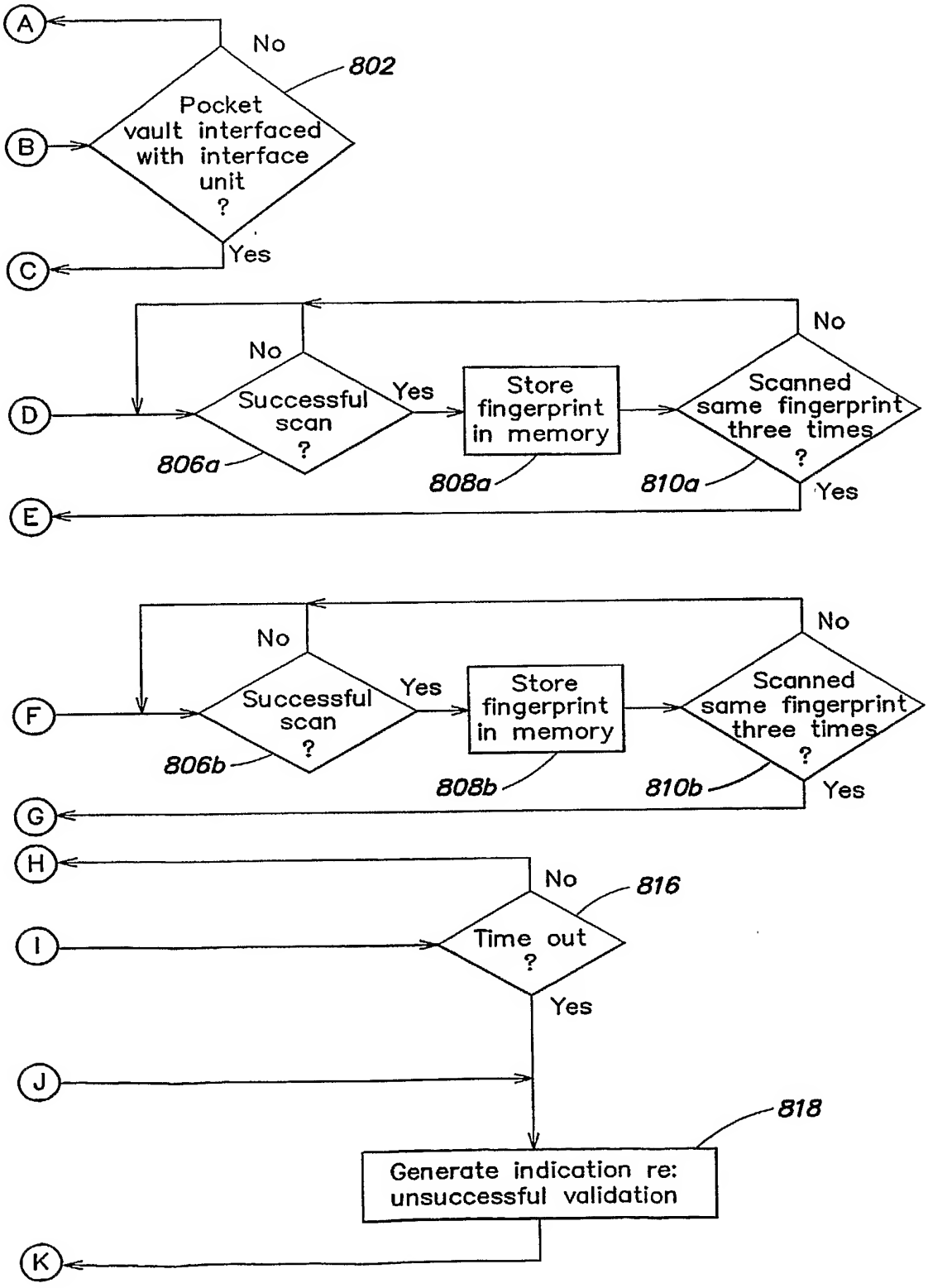

A
No
802
Pocket vault interfaced with interface unit ?
B
Yes
C
No
Successful scan ?
Yes
Store fingerprint in memory
Scanned same fingerprint three times ?
No
Yes
D
806a
808a
810a
E
No
Successful scan ?
Yes
Store fingerprint in memory
Scanned same fingerprint three times ?
No
Yes
F
806b
808b
810b
G
H
No
816
Time out ?
I
Yes
J
818
Generate indication re: unsuccessful validation
K

FIG. 8B

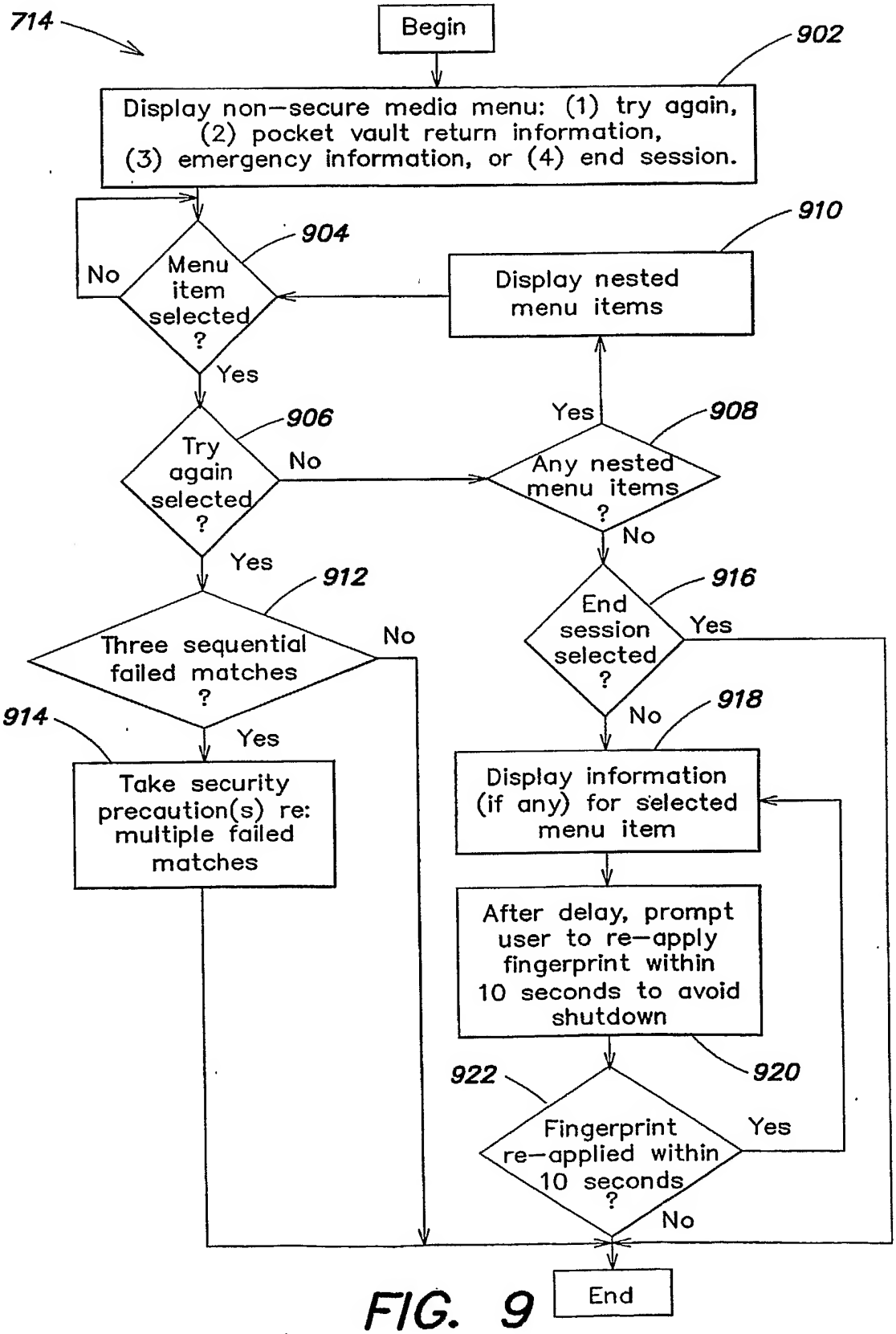

714
Begin
902
Display non-secure media menu: (1) try again, (2) pocket vault return information, (3) emergency information, or (4) end session.
904
Menu item selected ?
No
Yes
910
Display nested menu items
906
Try again selected ?
No
Yes
908
Any nested menu items ?
Yes
No
912
Three sequential failed matches ?
No
Yes
914
Take security precaution(s) re: multiple failed matches
916
End session selected ?
Yes
No
918
Display information (if any) for selected menu item
After delay, prompt user to re-apply fingerprint within 10 seconds to avoid shutdown
920
922
Fingerprint re-applied within 10 seconds ?
Yes
No
End

FIG. 9

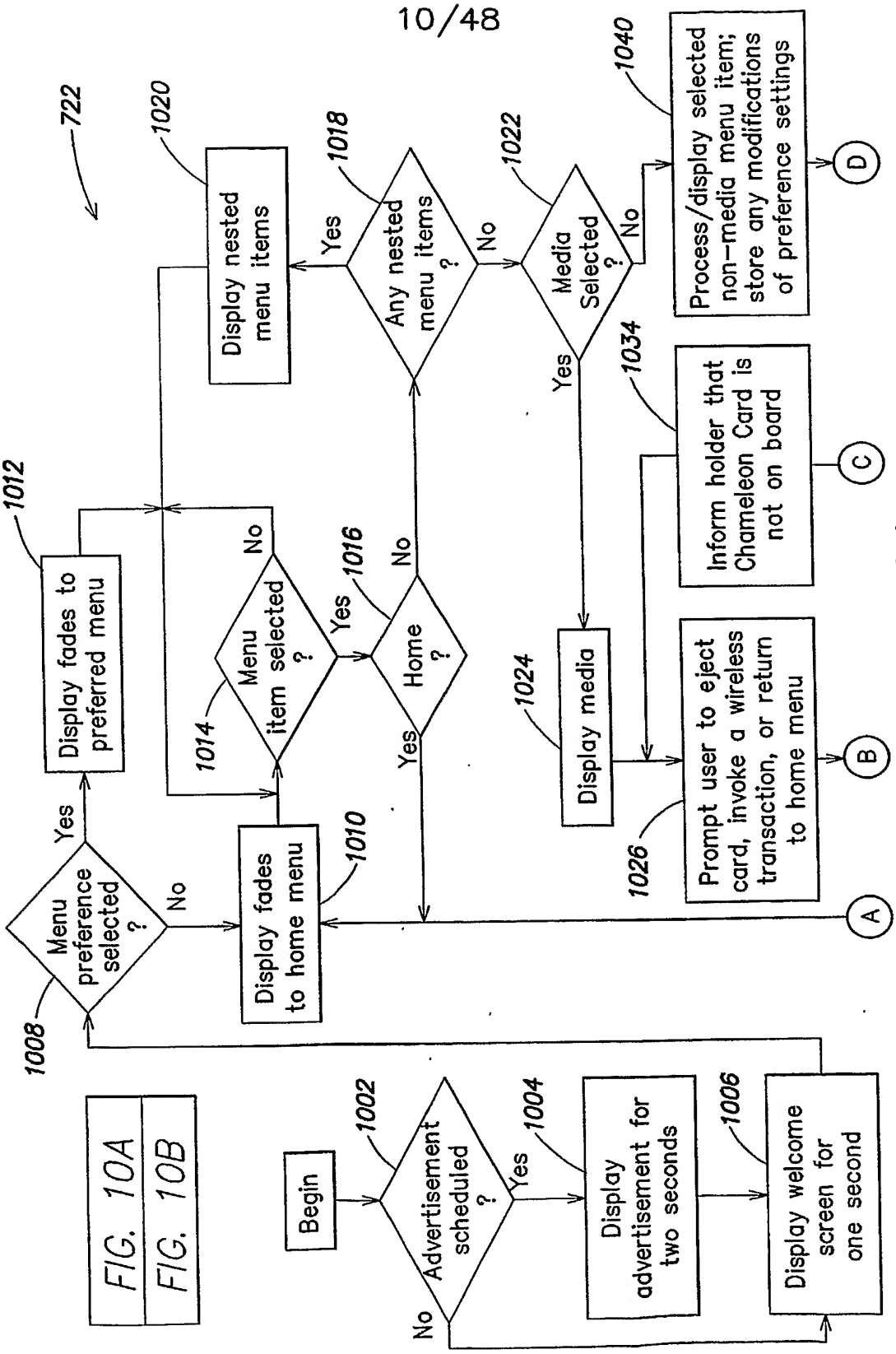


FIG. 10A

FIG. 10A
FIG. 10B

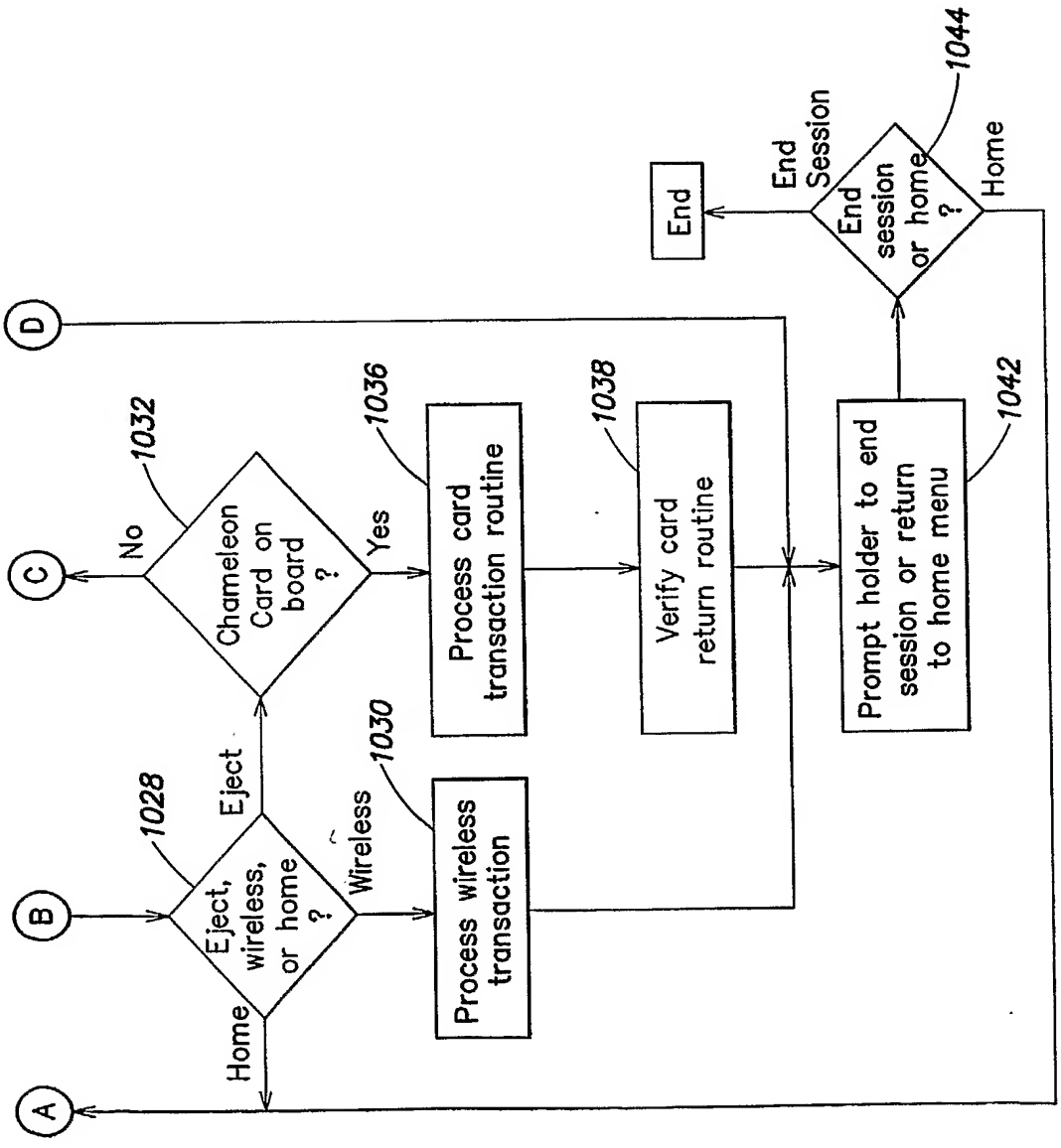

A
B
C
D
Eject, wireless, or home ?
1028
Eject
Wireless
Home
Chameleon Card on board ?
1032
No
Yes
Process wireless transaction
1030
Process card transaction routine
1036
Verify card return routine
1038
Prompt holder to end session or return to home menu
1042
End session or home ?
1044
End Session
Home
End

FIG. 10B

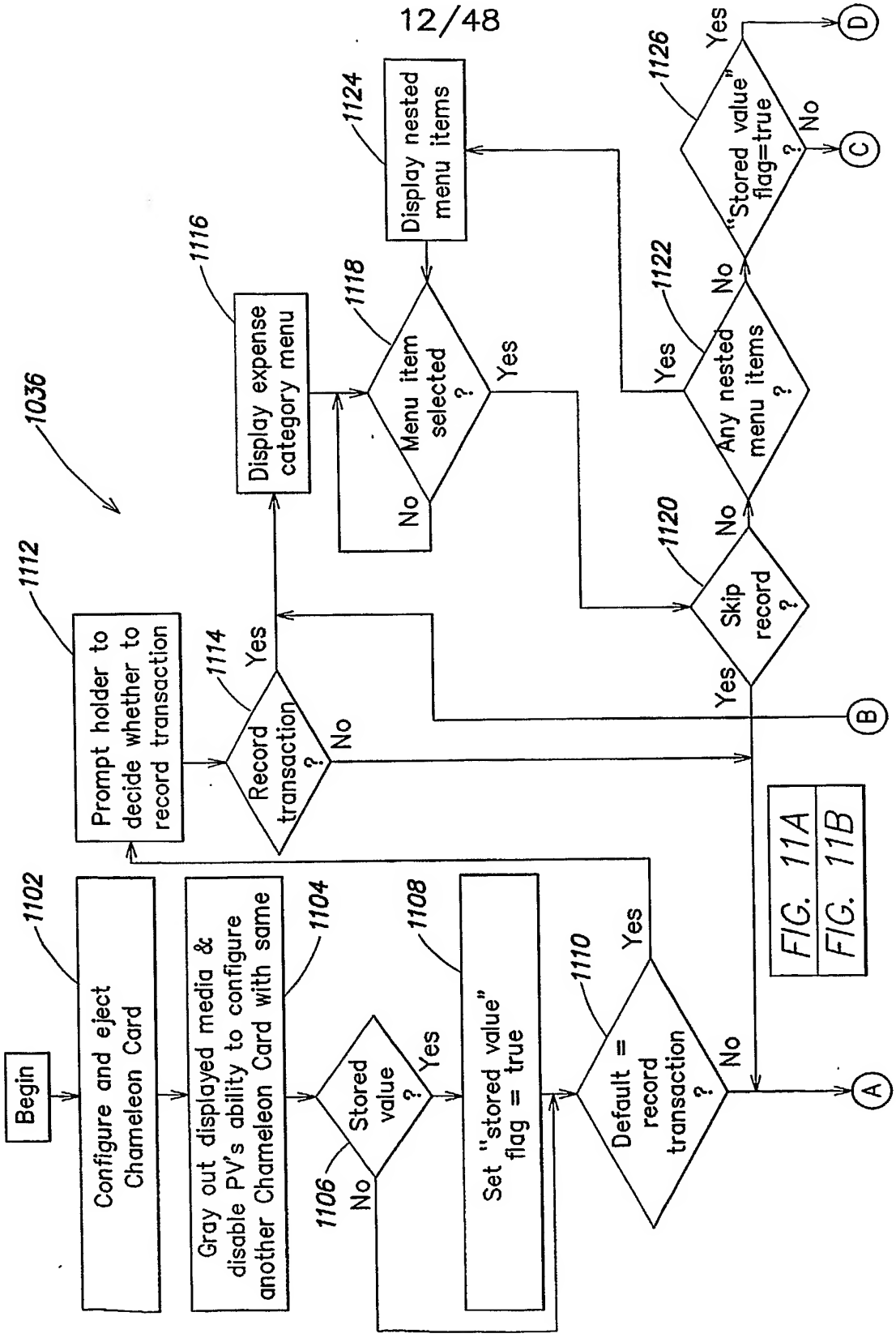


FIG. 11A

FIG. 11A
FIG. 11B

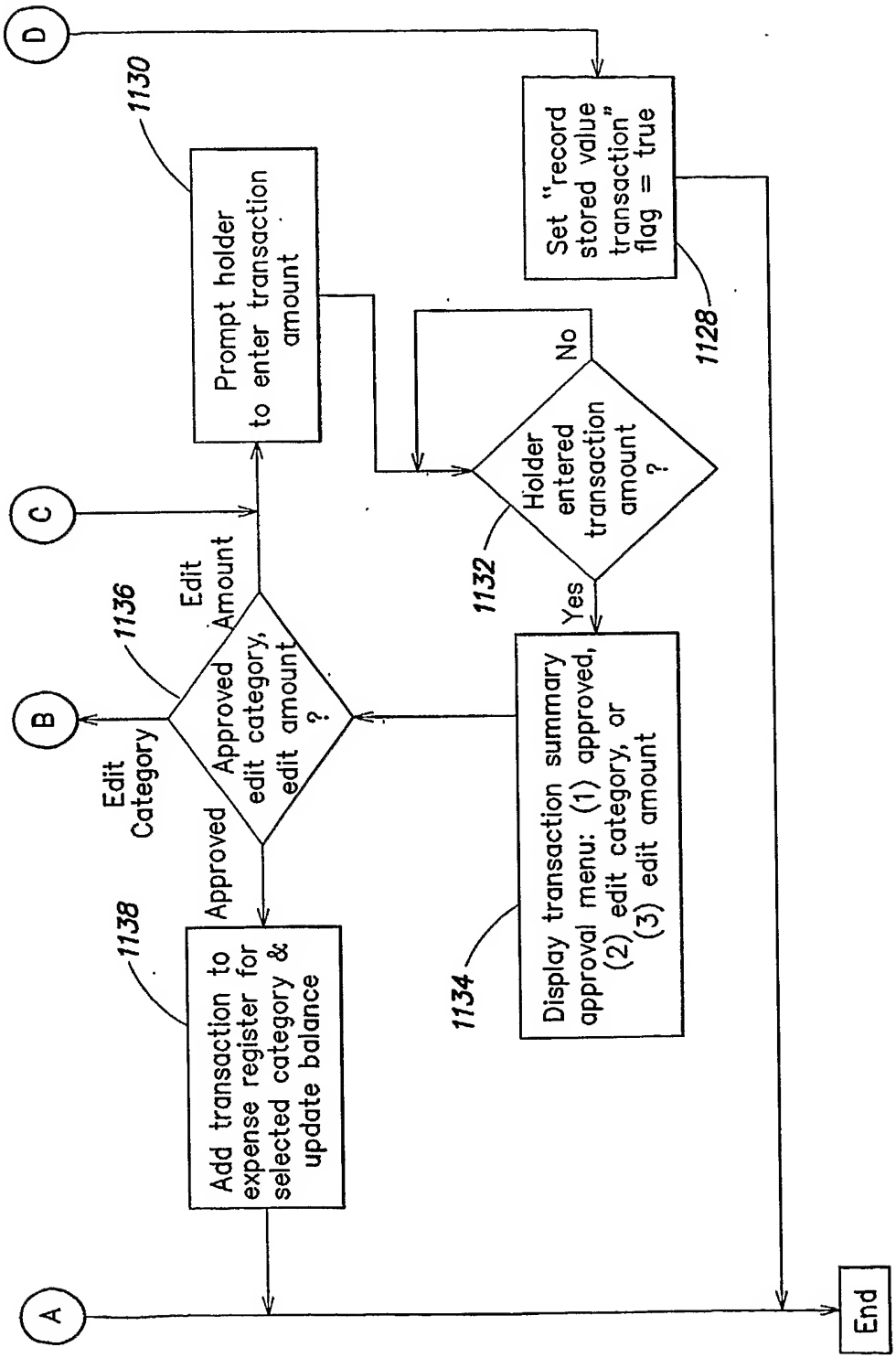

D
1130
Prompt holder to enter transaction amount
Set "record stored value transaction" flag = true
1128
No
Holder entered transaction amount ?
1132
Yes
C
Edit Amount
1136
Approved edit category, edit amount ?
B
Edit Category
Approved
1138
Add transaction to expense register for selected category & update balance
1134
Display transaction summary approval menu: (1) approved, (2) edit category, or (3) edit amount
A
End

FIG. 11B

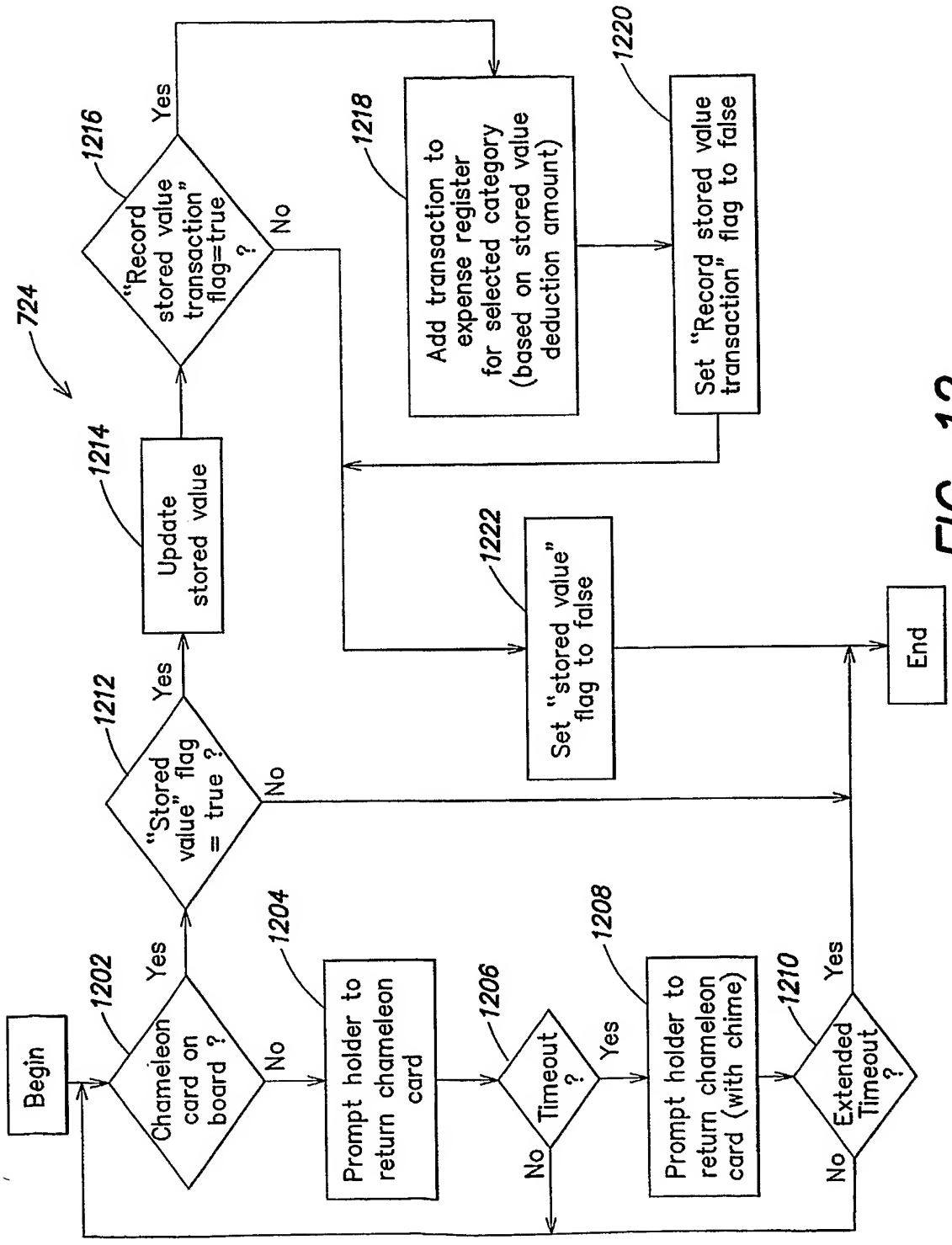

724
Begin
1202
Chameleon card on board ?
Yes
No
1204
Prompt holder to return chameleon card
1206
Timeout ?
No
Yes
1208
Prompt holder to return chameleon card (with chime)
1210
Extended Timeout ?
No
Yes
1212
"Stored value" flag = true ?
Yes
No
1214
Update stored value
1216
"Record stored value transaction" flag=true ?
Yes
No
1218
Add transaction to expense register for selected category (based on stored value deduction amount)
1220
Set "Record stored value transaction" flag to false
1222
Set "stored value" flag to false
End

FIG. 12

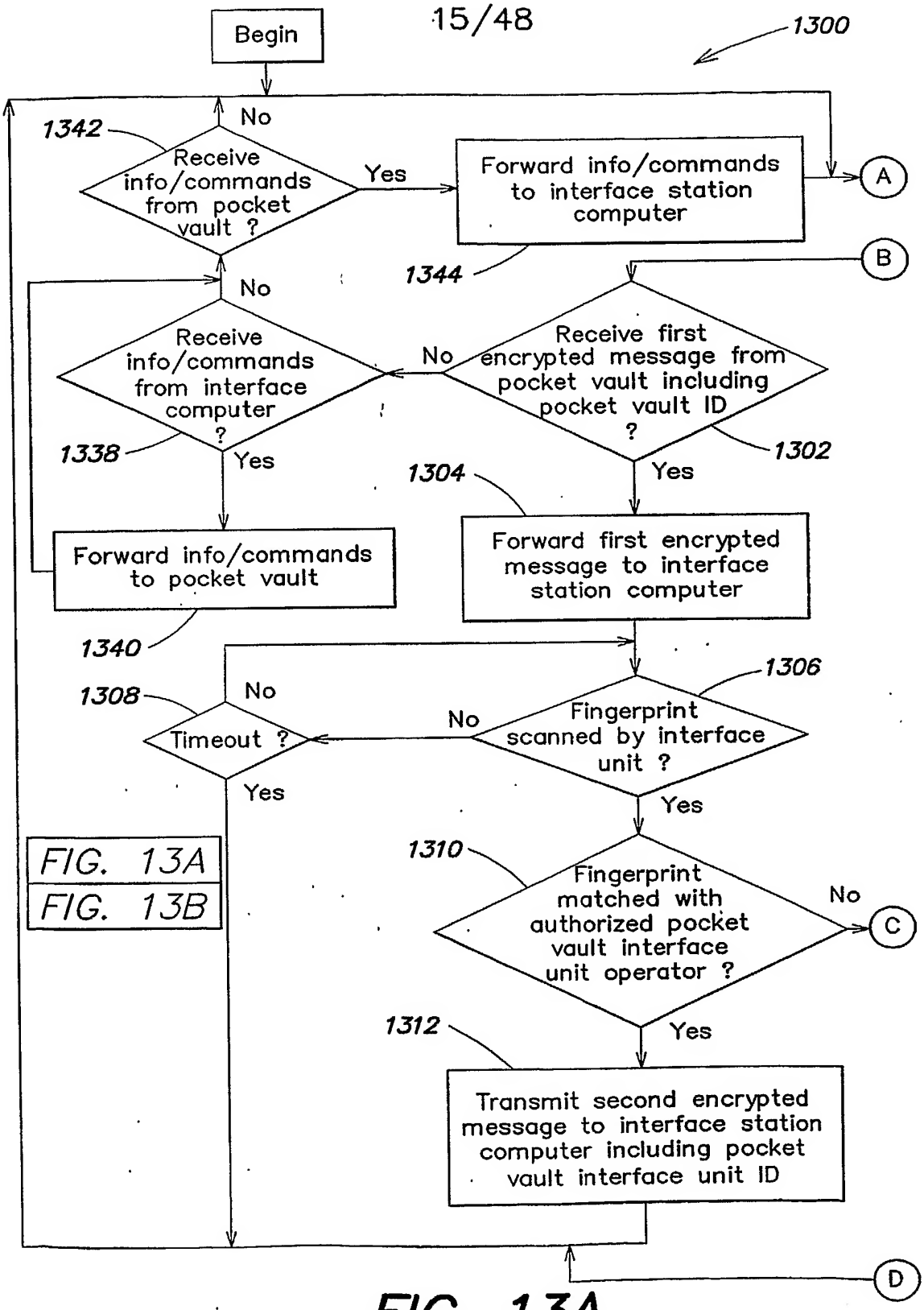


FIG. 13A
FIG. 13B

FIG. 13A

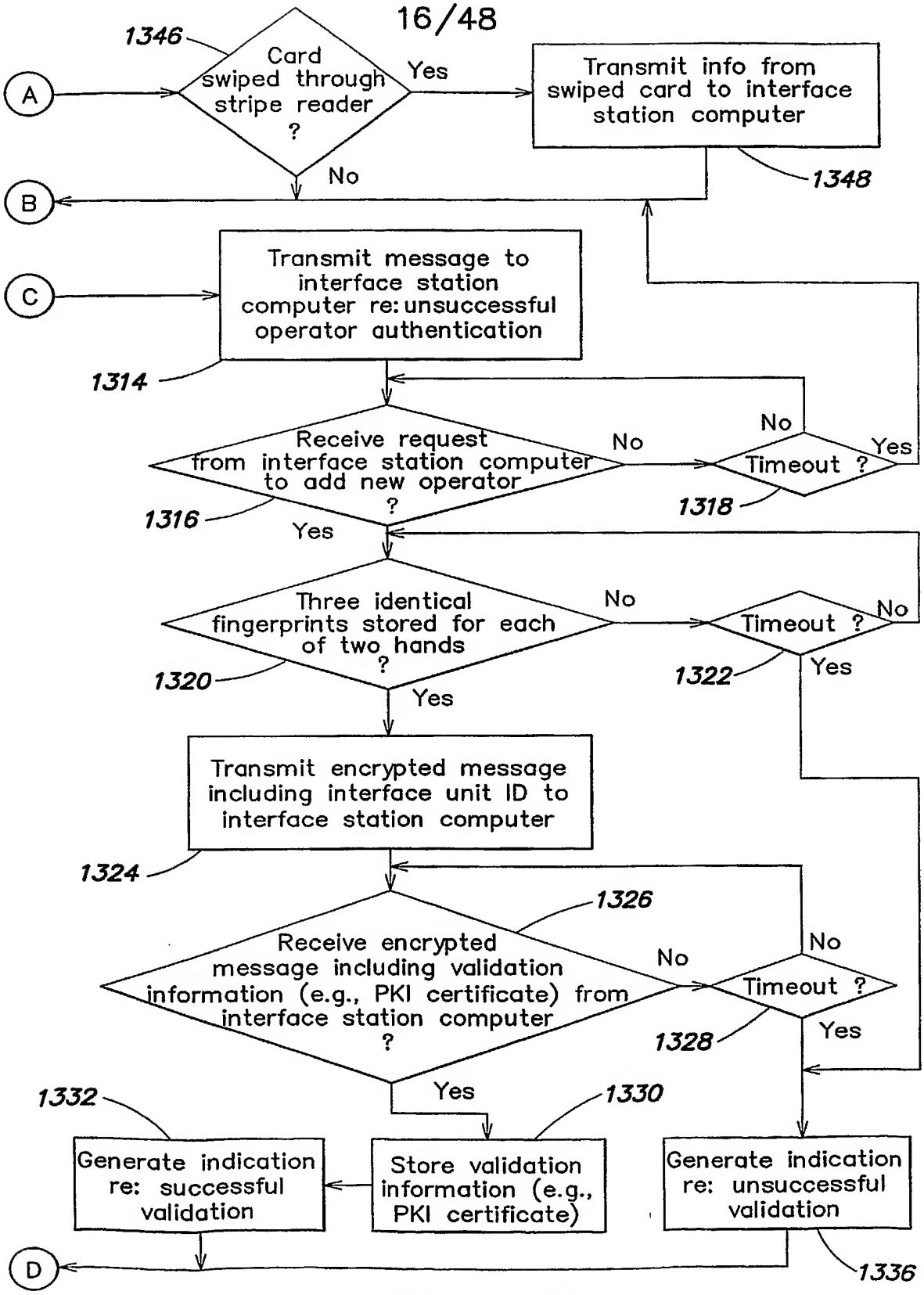

1346
Card swiped through stripe reader ?
Yes
No
A
B
Transmit info from swiped card to interface station computer
1348
C
Transmit message to interface station computer re: unsuccessful operator authentication
1314
Receive request from interface station computer to add new operator ?
1316
No
Yes
Timeout ?
1318
No
Yes
Three identical fingerprints stored for each of two hands ?
1320
No
Yes
Timeout ?
1322
No
Yes
Transmit encrypted message including interface unit ID to interface station computer
1324
1326
Receive encrypted message including validation information (e.g., PKI certificate) from interface station computer ?
No
Yes
Timeout ?
1328
No
Yes
1332
1330
Generate indication re: successful validation
Store validation information (e.g., PKI certificate)
Generate indication re: unsuccessful validation
1336
D

FIG. 13B

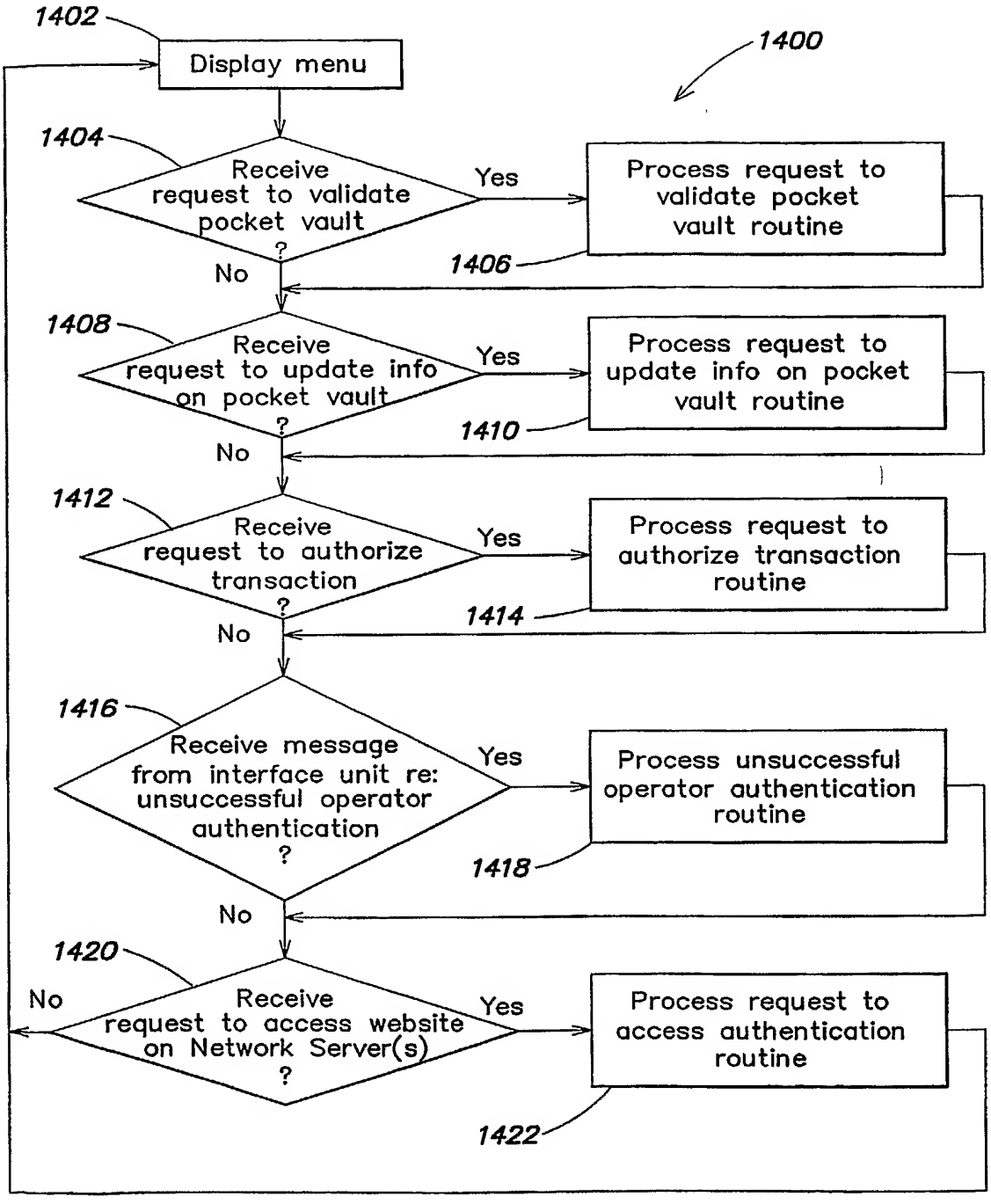

1402
Display menu
1400
1404
Receive request to validate pocket vault ?
Yes
Process request to validate pocket vault routine
1406
No
1408
Receive request to update info on pocket vault ?
Yes
Process request to update info on pocket vault routine
1410
No
1412
Receive request to authorize transaction ?
Yes
Process request to authorize transaction routine
1414
No
1416
Receive message from interface unit re: unsuccessful operator authentication ?
Yes
Process unsuccessful operator authentication routine
1418
No
1420
No
Receive request to access website on Network Server(s) ?
Yes
Process request to access authentication routine
1422

FIG. 14

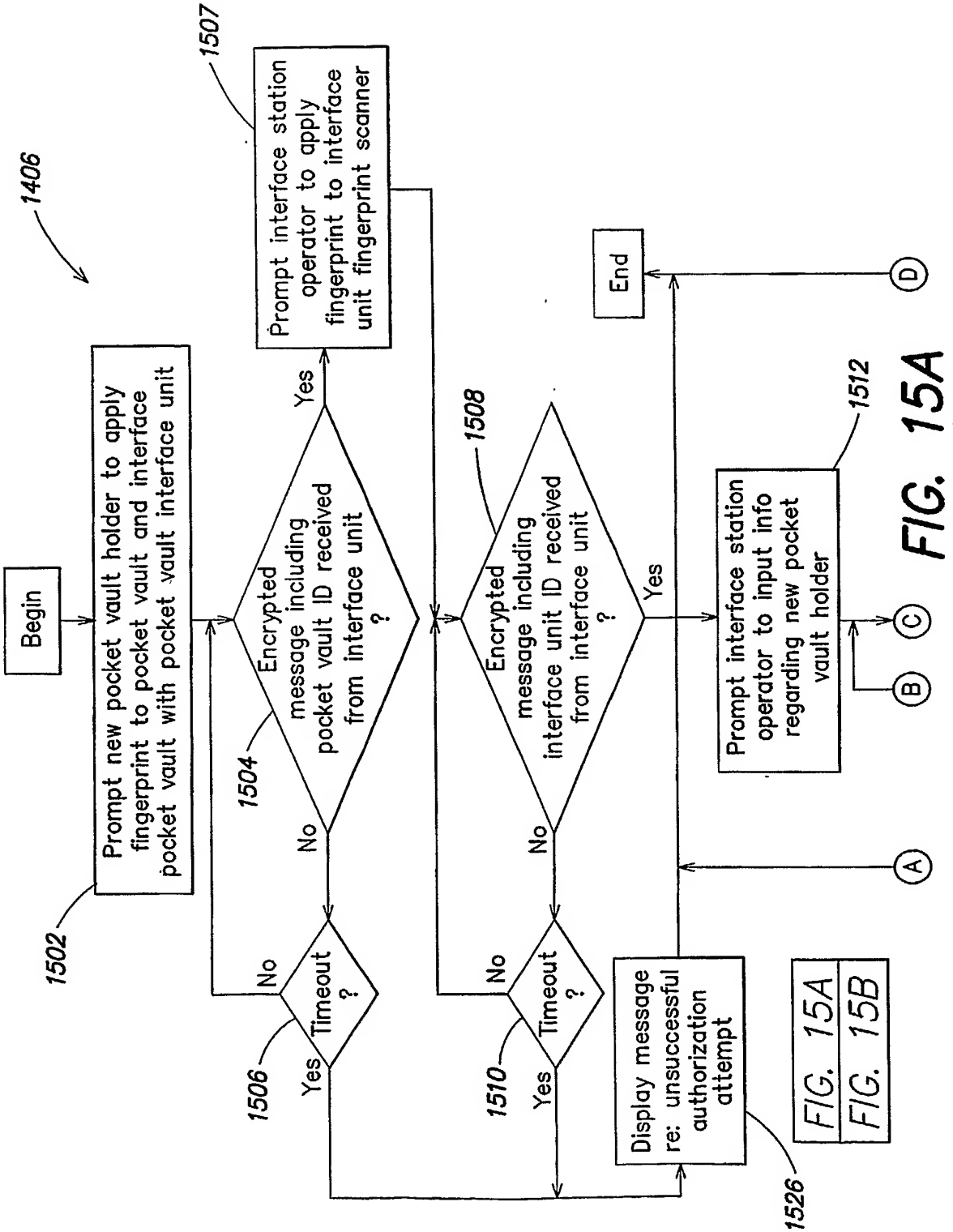


FIG. 15A

FIG. 15A
FIG. 15B

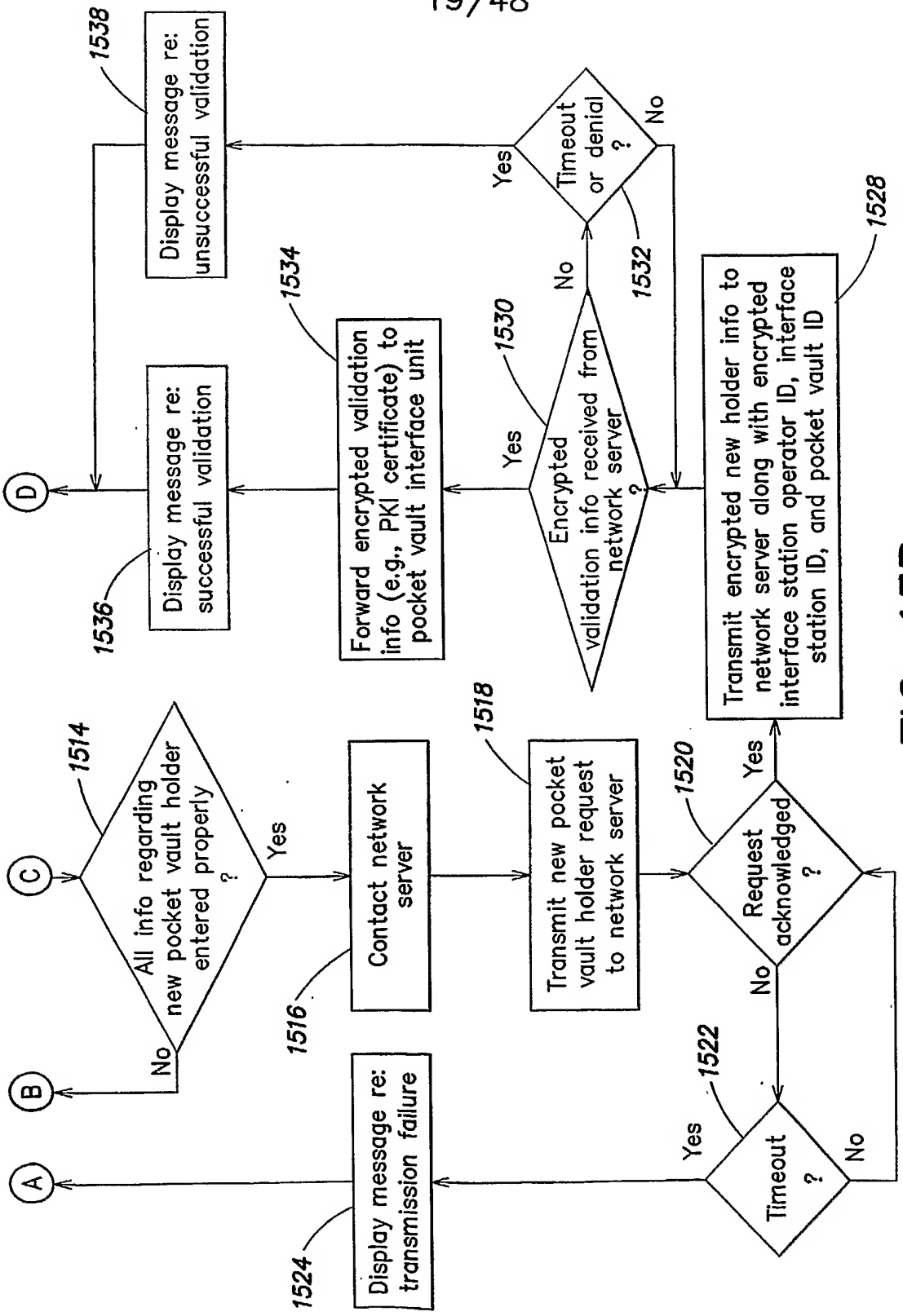

A
B
C
D
All info regarding new pocket vault holder entered properly ?
1514
No
Yes
Contact network server
1516
Transmit new pocket vault holder request to network server
1518
Request acknowledged ?
1520
Yes
No
Timeout ?
1522
Yes
No
Display message re: transmission failure
1524
Transmit encrypted new holder info to network server along with encrypted interface station operator ID, interface station ID, and pocket vault ID
1528
Encrypted validation info received from network server ?
1530
No
Yes
Timeout or denial ?
1532
Yes
No
Forward encrypted validation info (e.g., PKI certificate) to pocket vault interface unit
1534
Display message re: successful validation
1536
Display message re: unsuccessful validation
1538

FIG. 15B

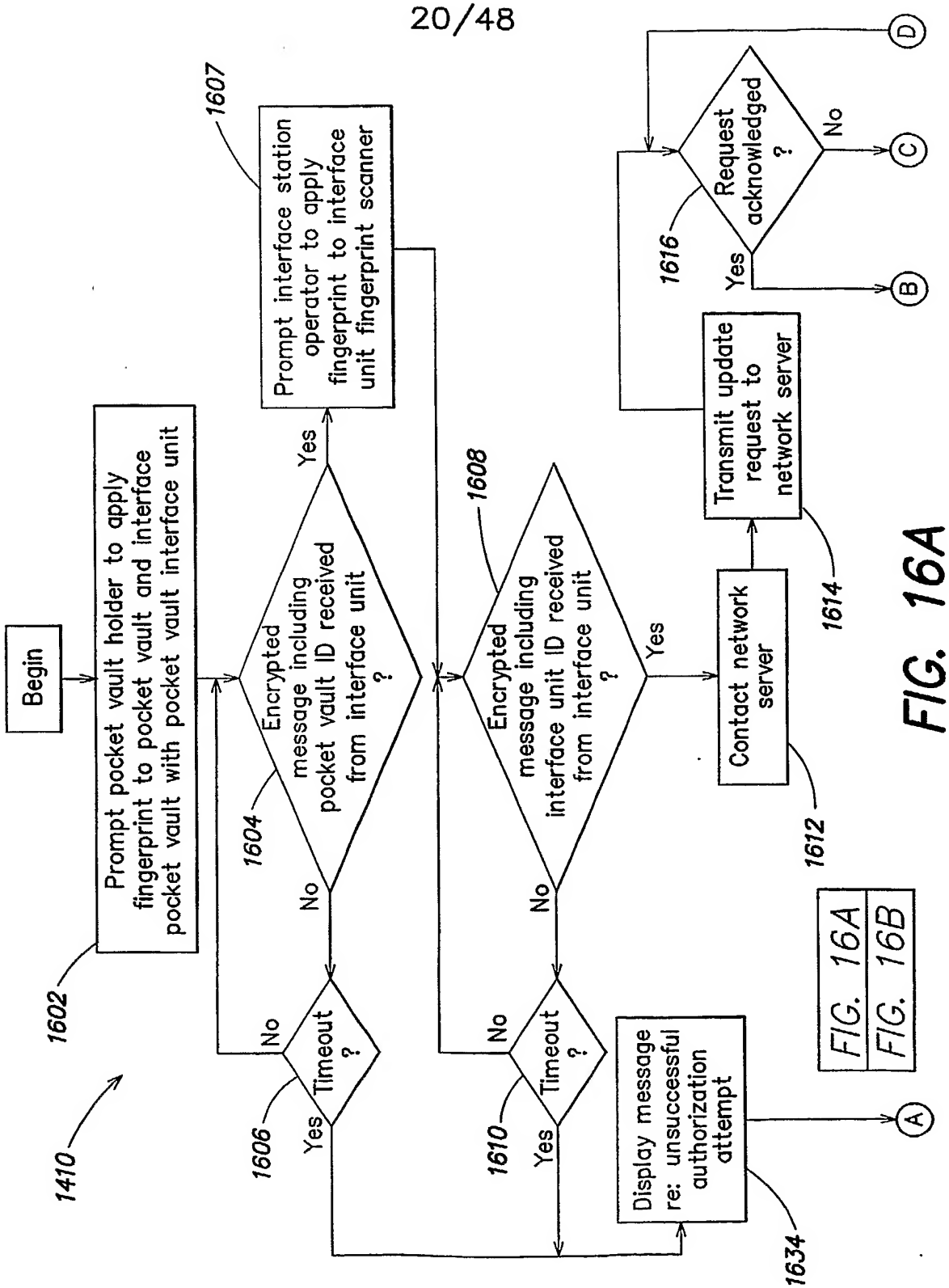


FIG. 16A

FIG. 16A
FIG. 16B

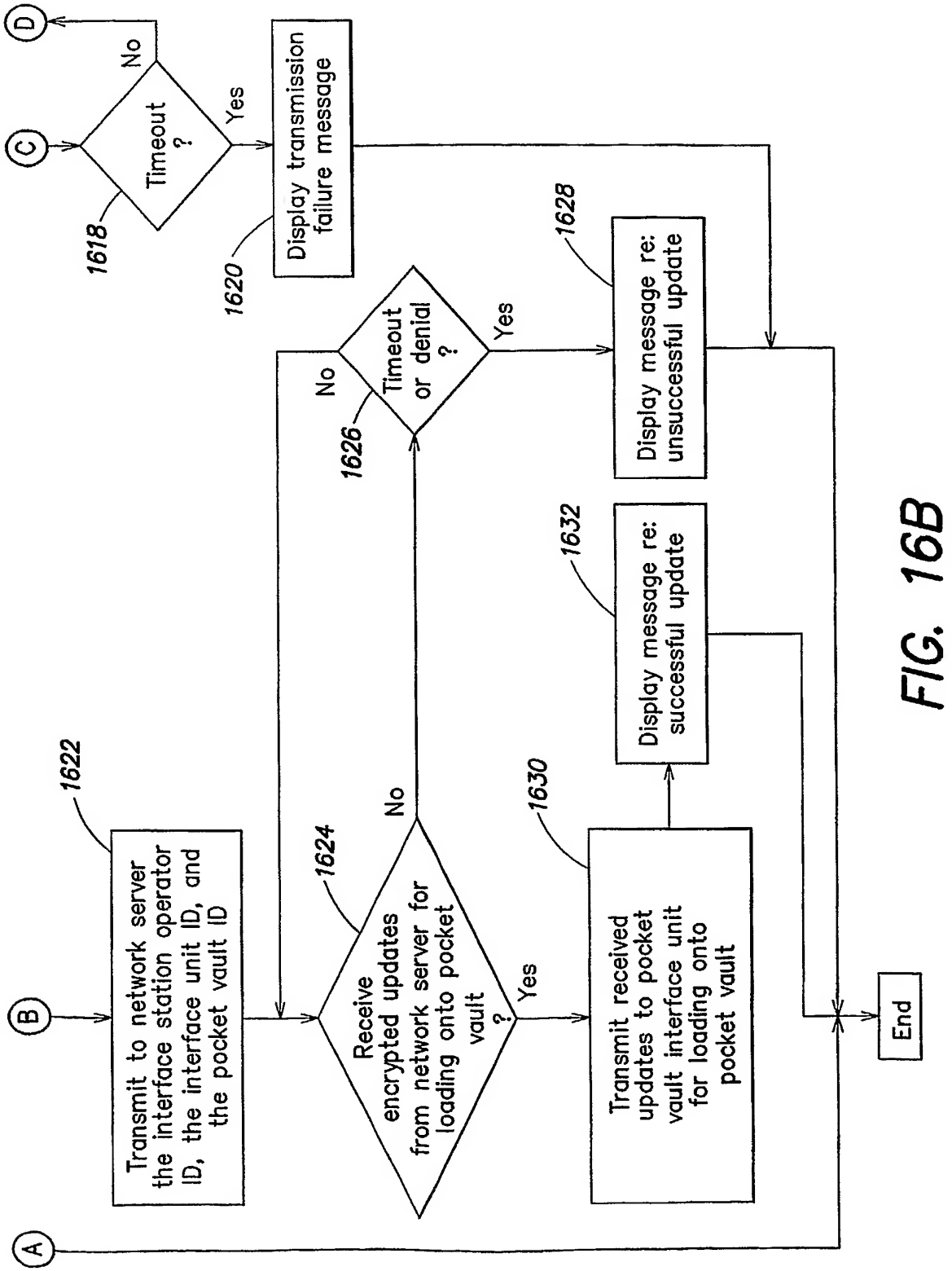

A
B
C
D
Transmit to network server the interface station operator ID, the interface unit ID, and the pocket vault ID
1622
Receive encrypted updates from network server for loading onto pocket vault ?
1624
No
Yes
Timeout ?
1618
No
Yes
Display transmission failure message
1620
Timeout or denial ?
1626
No
Yes
Display message re: unsuccessful update
1628
Transmit received updates to pocket vault interface unit for loading onto pocket vault
1630
Display message re: successful update
1632
End

FIG. 16B

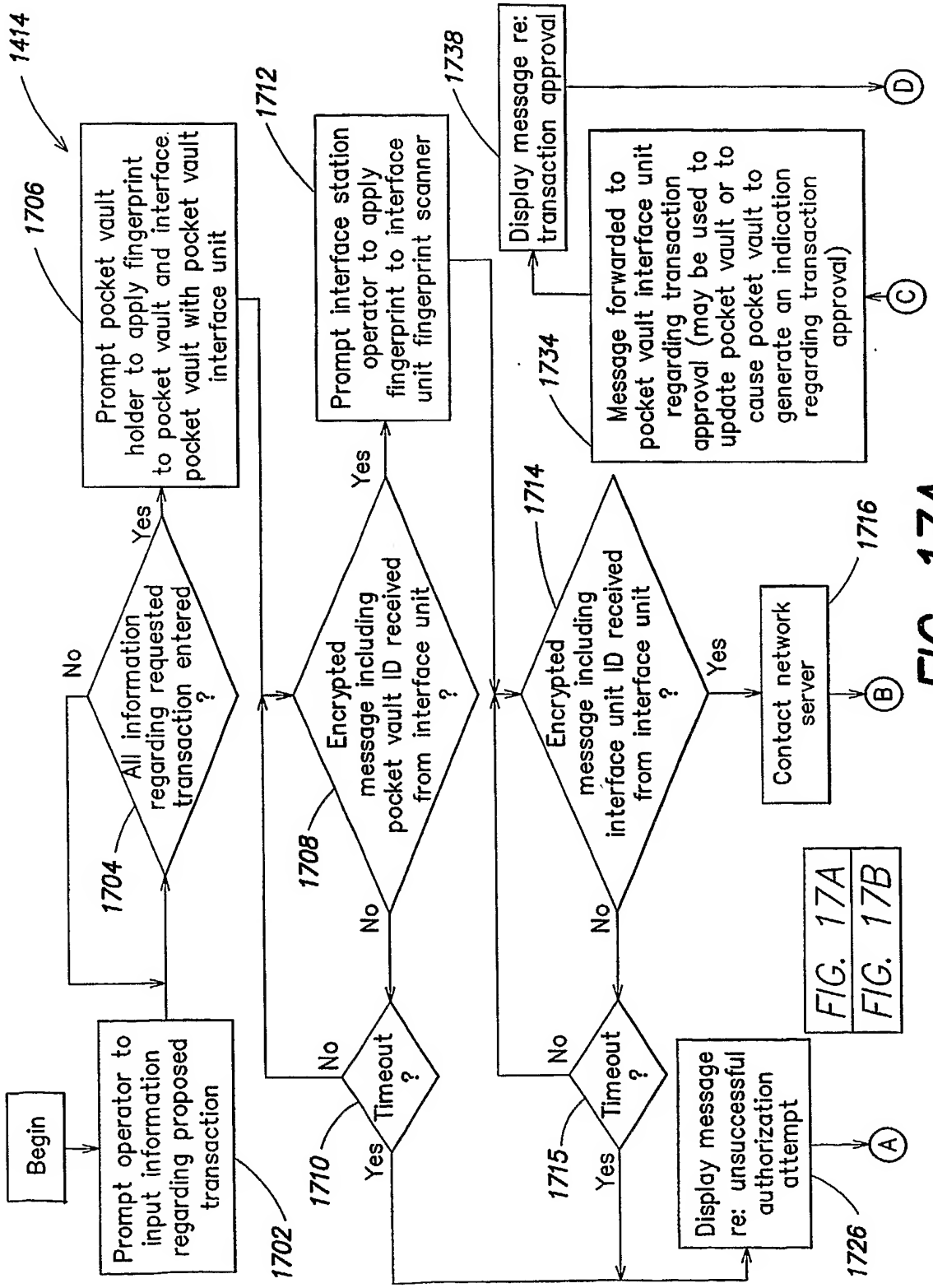


FIG. 17A

FIG. 17A
FIG. 17B

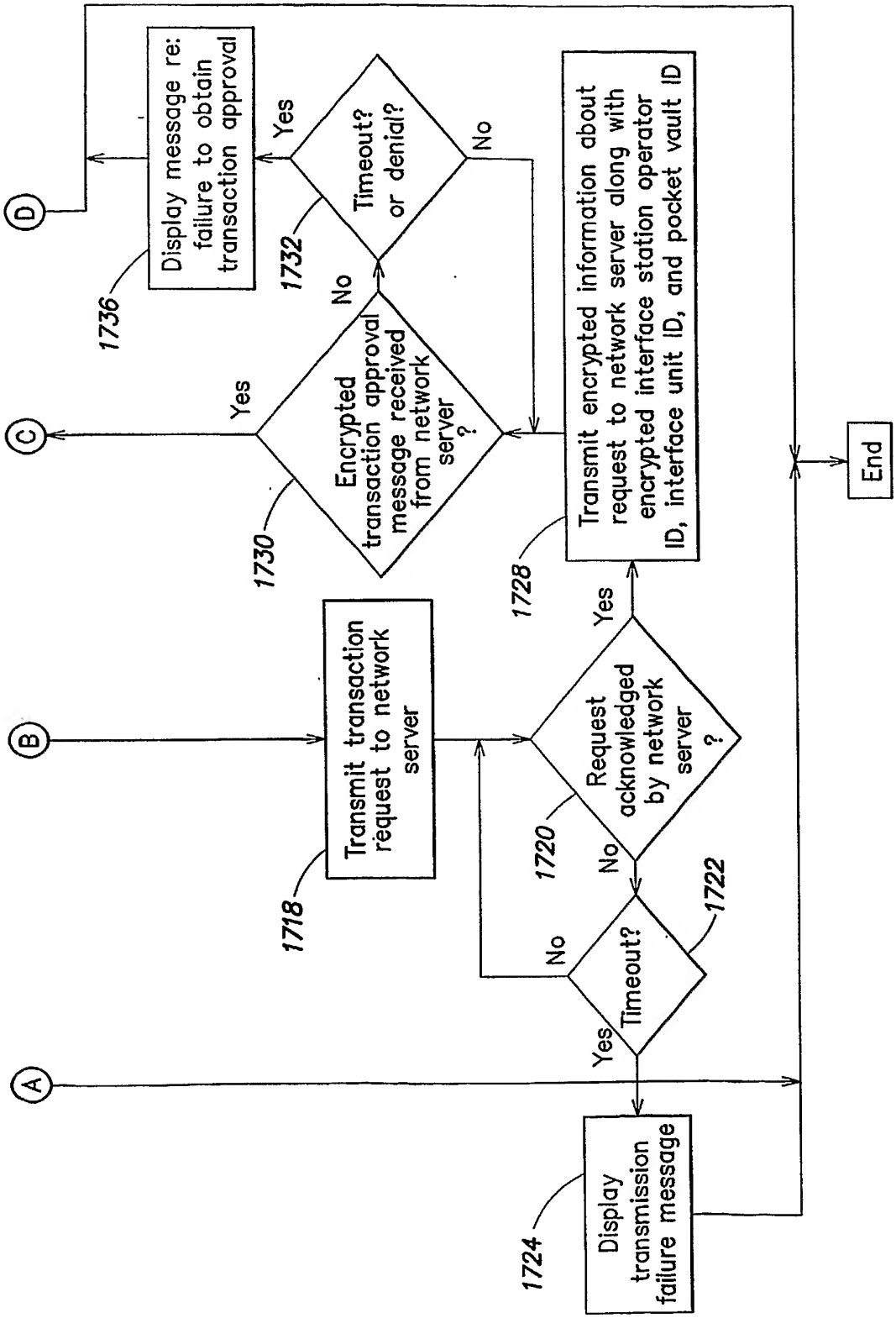

A
B
C
D
Transmit transaction request to network server
1718
Request acknowledged by network server ?
1720
Yes
No
Timeout?
1722
Yes
No
Display transmission failure message
1724
Transmit encrypted information about request to network server along with encrypted interface station operator ID, interface unit ID, and pocket vault ID
1728
Encrypted transaction approval message received from network server ?
1730
Yes
No
Timeout? or denial?
1732
Yes
No
Display message re: failure to obtain transaction approval
1736
End

FIG. 17B

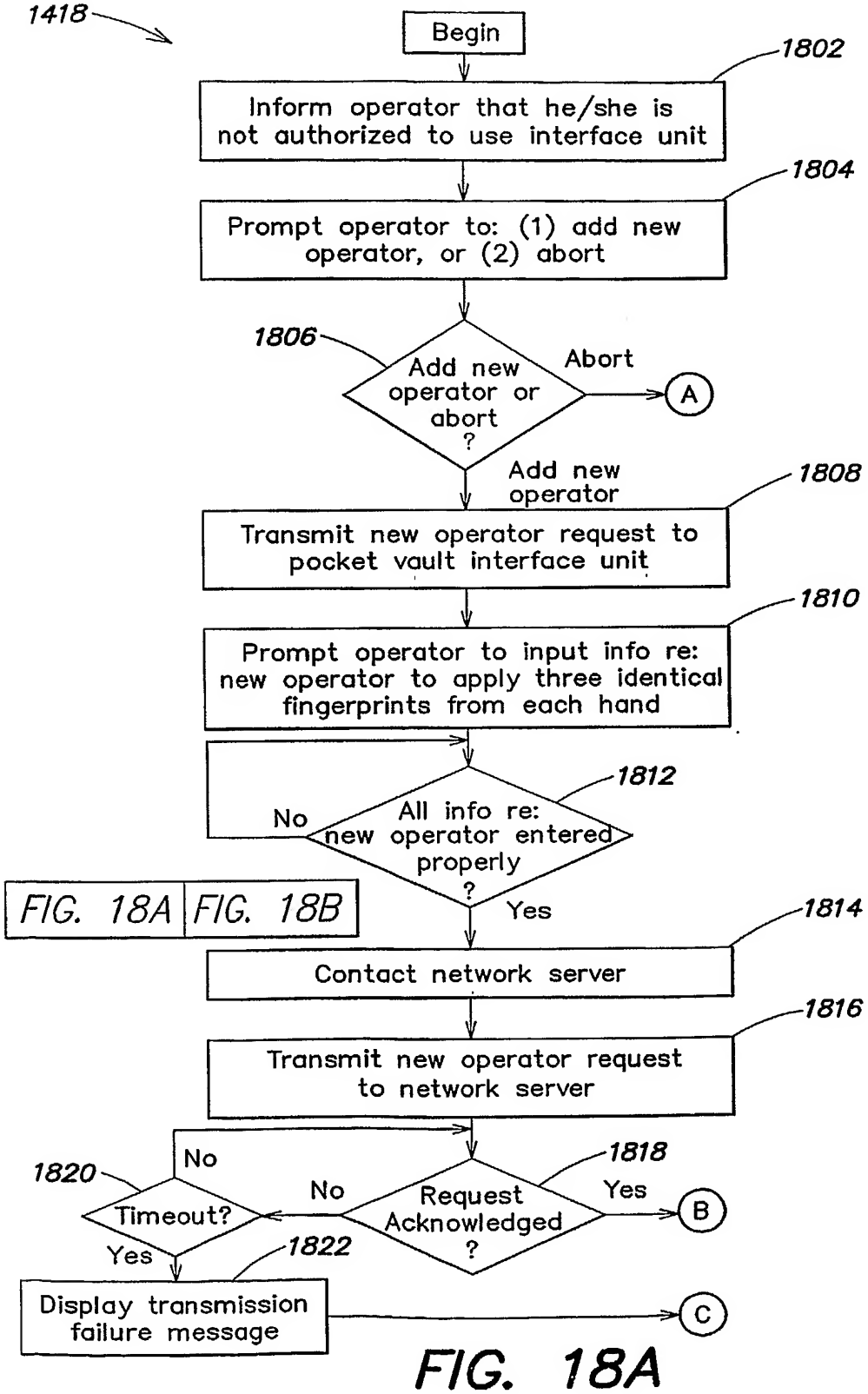


FIG. 18A | FIG. 18B

FIG. 18A

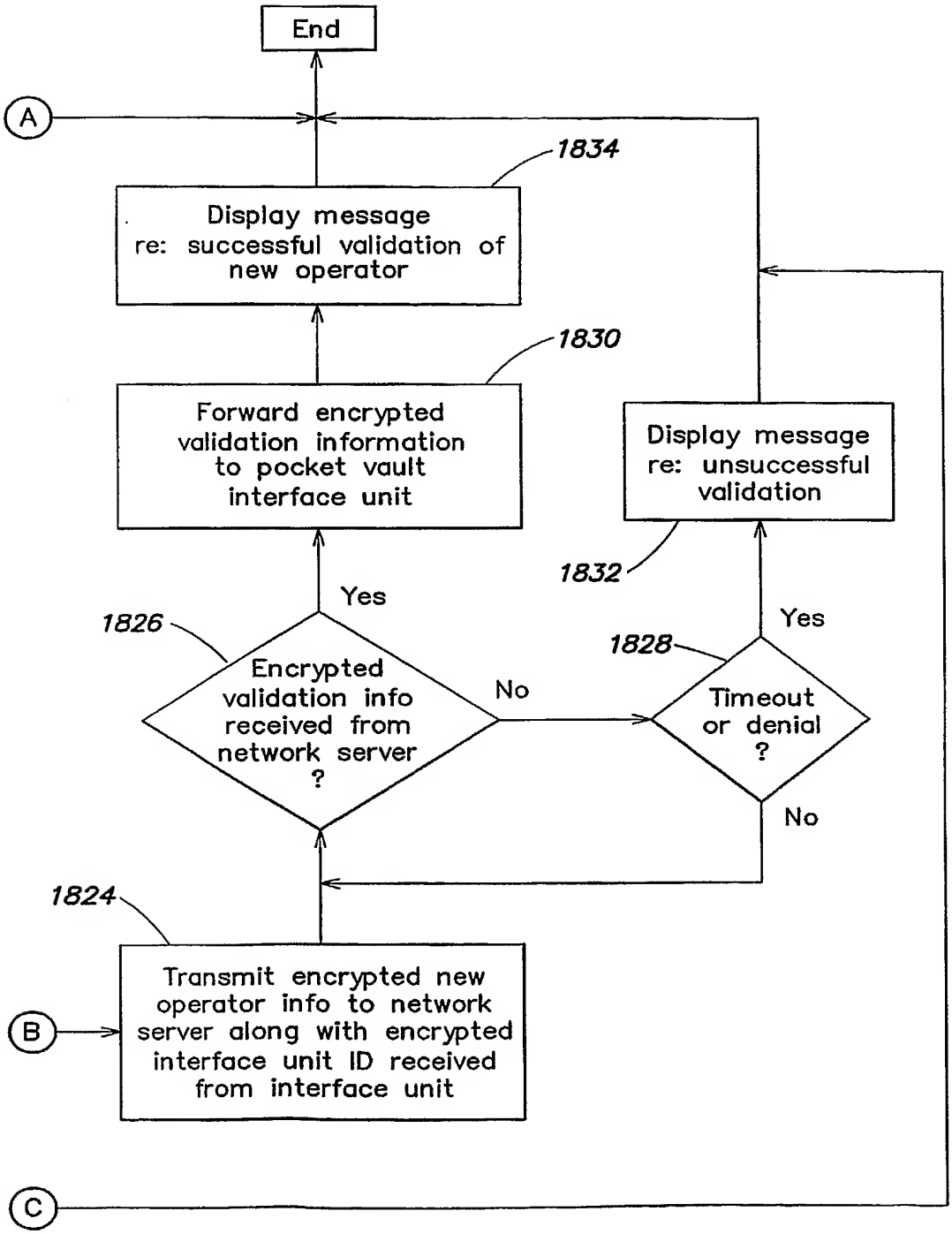

End
A
1834
Display message re: successful validation of new operator
1830
Forward encrypted validation information to pocket vault interface unit
Display message re: unsuccessful validation
1832
Yes
1826
Encrypted validation info received from network server ?
No
1828
Timeout or denial ?
Yes
No
1824
Transmit encrypted new operator info to network server along with encrypted interface unit ID received from interface unit
B
C

FIG. 18B

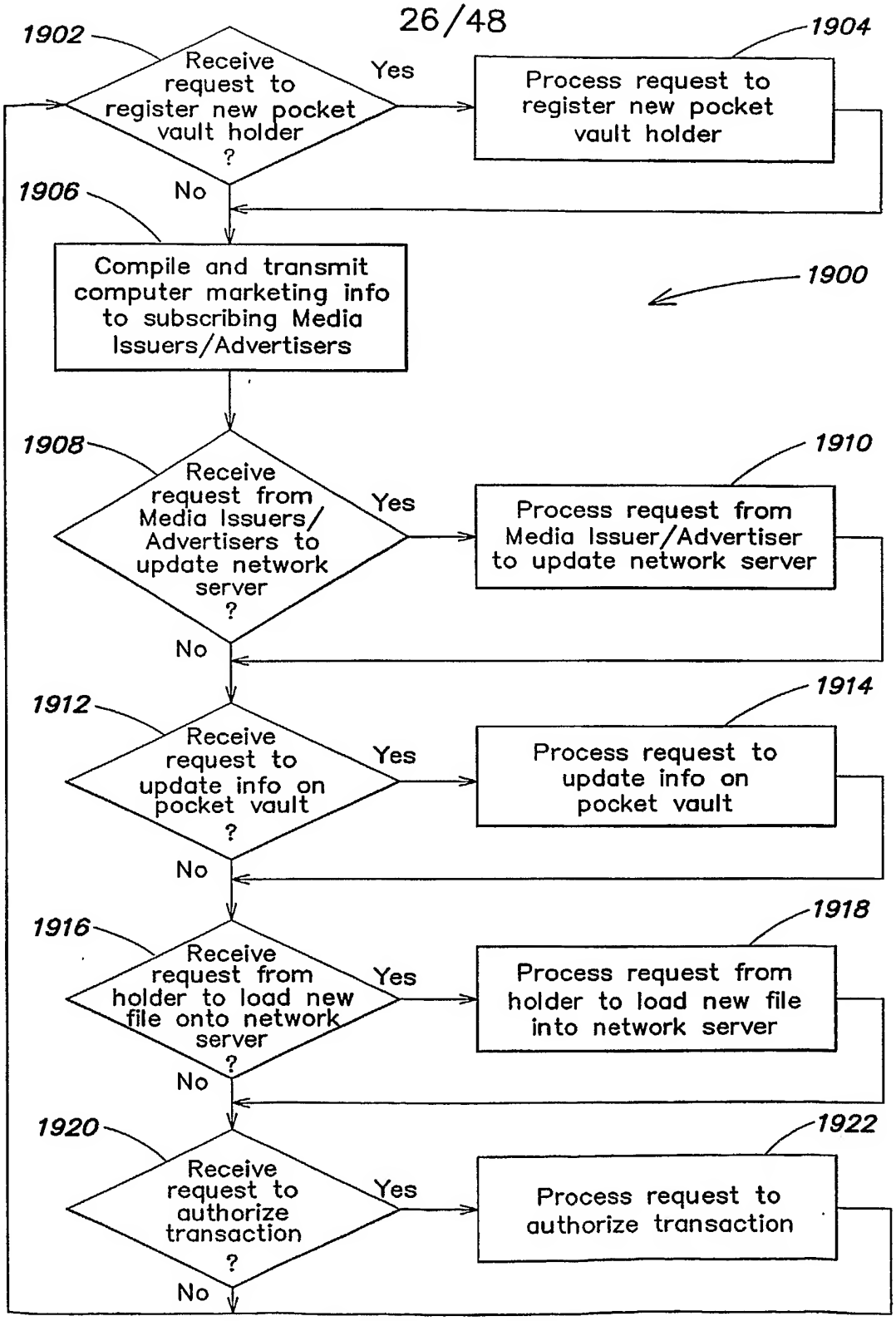

1902
Receive request to register new pocket vault holder ?
Yes
1904
Process request to register new pocket vault holder
No
1906
Compile and transmit computer marketing info to subscribing Media Issuers/Advertisers
1900
1908
Receive request from Media Issuers/ Advertisers to update network server ?
Yes
1910
Process request from Media Issuer/Advertiser to update network server
No
1912
Receive request to update info on pocket vault ?
Yes
1914
Process request to update info on pocket vault
No
1916
Receive request from holder to load new file onto network server ?
Yes
1918
Process request from holder to load new file into network server
No
1920
Receive request to authorize transaction ?
Yes
1922
Process request to authorize transaction
No

FIG. 19

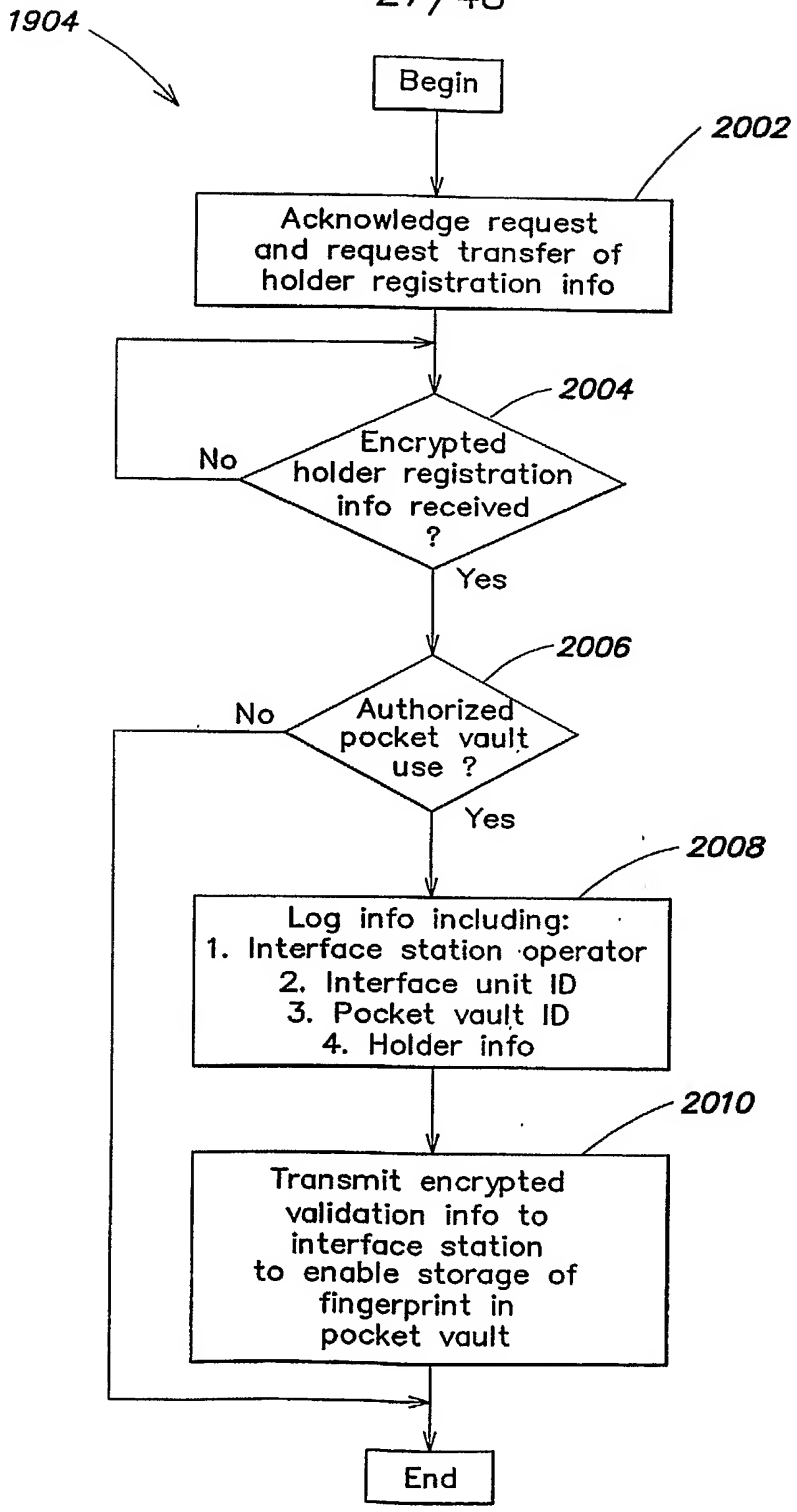

1904
Begin
2002
Acknowledge request and request transfer of holder registration info
2004
Encrypted holder registration info received ?
No
Yes
2006
Authorized pocket vault use ?
No
Yes
2008
Log info including:
1. Interface station operator
2. Interface unit ID
3. Pocket vault ID
4. Holder info
2010
Transmit encrypted validation info to interface station to enable storage of fingerprint in pocket vault
End

FIG. 20

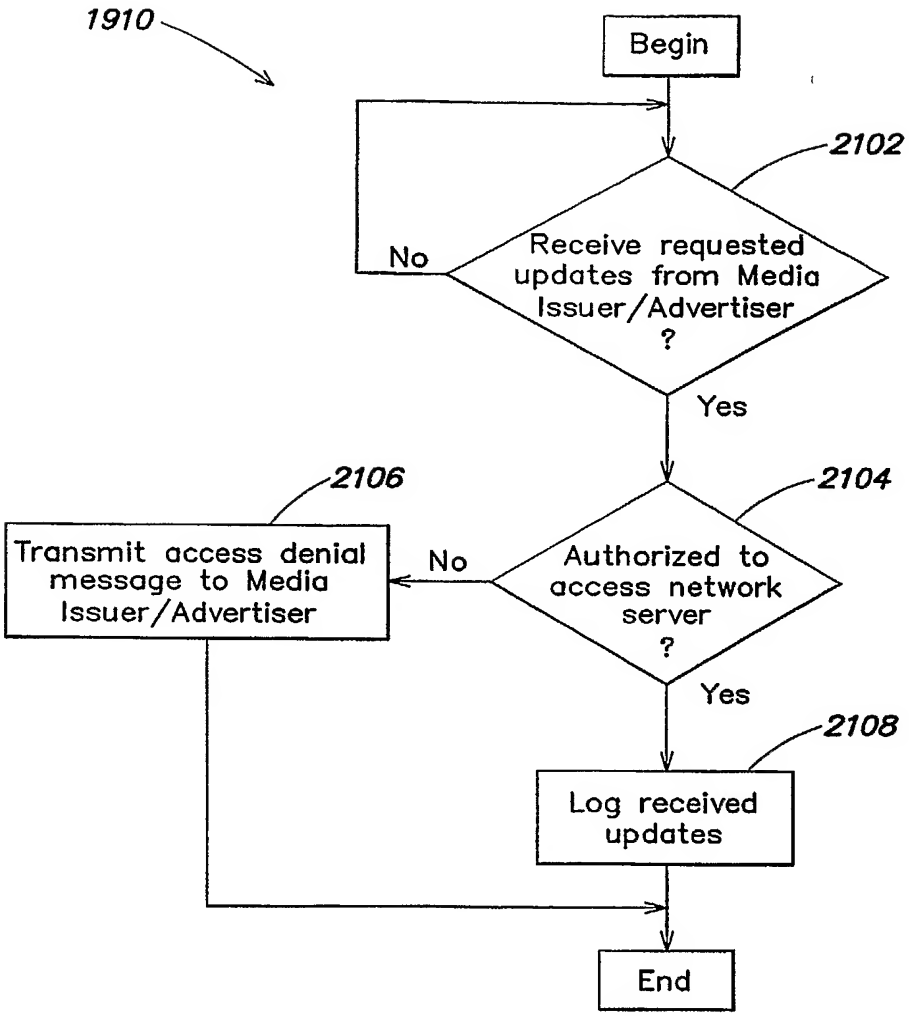

1910
Begin
2102
Receive requested updates from Media Issuer/Advertiser ?
No
Yes
2104
Authorized to access network server ?
No
2106
Transmit access denial message to Media Issuer/Advertiser
Yes
2108
Log received updates
End

FIG. 21

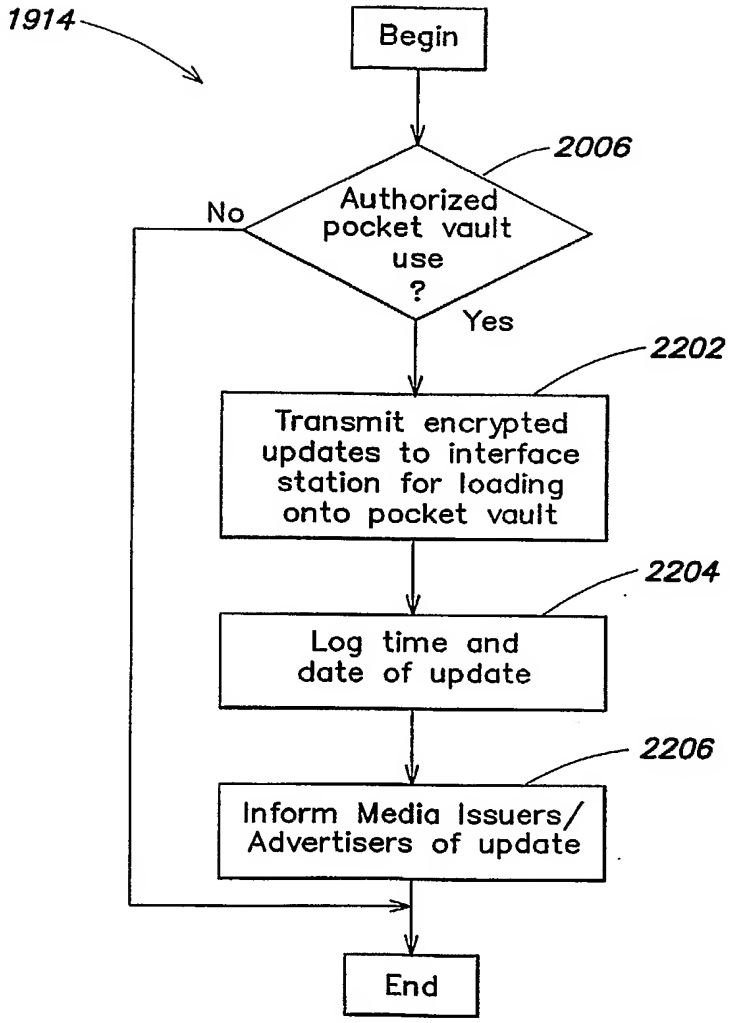

1914
Begin
2006
Authorized pocket vault use ?
No
Yes
2202
Transmit encrypted updates to interface station for loading onto pocket vault
2204
Log time and date of update
2206
Inform Media Issuers/ Advertisers of update
End

FIG. 22

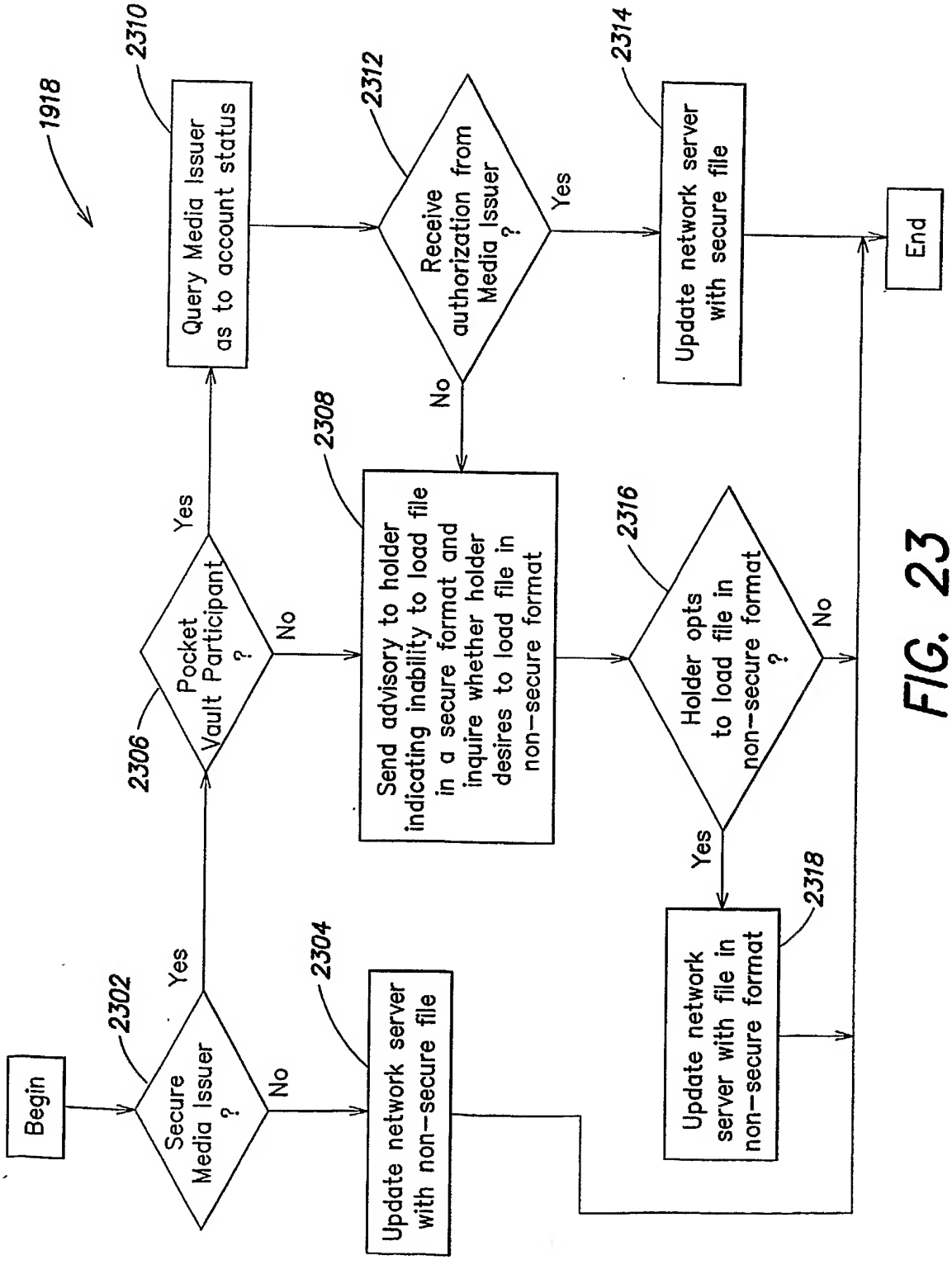

1918
Begin
2302
Secure Media Issuer ?
Yes
No
2304
Update network server with non-secure file
2306
Pocket Vault Participant ?
Yes
No
2308
Send advisory to holder indicating inability to load file in a secure format and inquire whether holder desires to load file in non-secure format
2310
Query Media Issuer as to account status
2312
Receive authorization from Media Issuer ?
Yes
No
2314
Update network server with secure file
2316
Holder opts to load file in non-secure format ?
Yes
No
2318
Update network server with file in non-secure format
End

FIG. 23

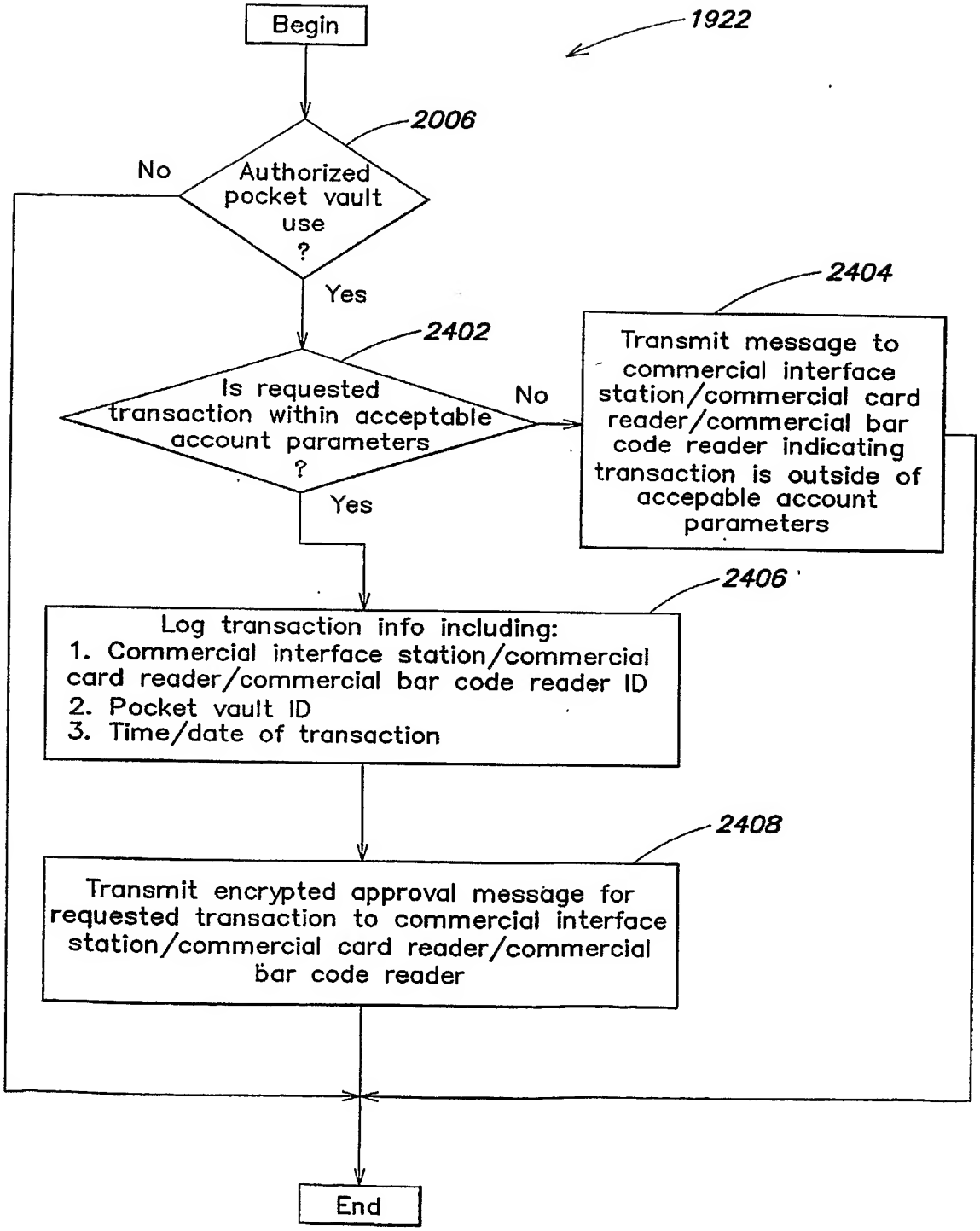

Begin
1922
2006
Authorized pocket vault use ?
No
Yes
2402
Is requested transaction within acceptable account parameters ?
No
Yes
2404
Transmit message to commercial interface station/commercial card reader/commercial bar code reader indicating transaction is outside of accepable account parameters
2406
Log transaction info including:
1. Commercial interface station/commercial card reader/commercial bar code reader ID
2. Pocket vault ID
3. Time/date of transaction
2408
Transmit encrypted approval message for requested transaction to commercial interface station/commercial card reader/commercial bar code reader
End

FIG. 24

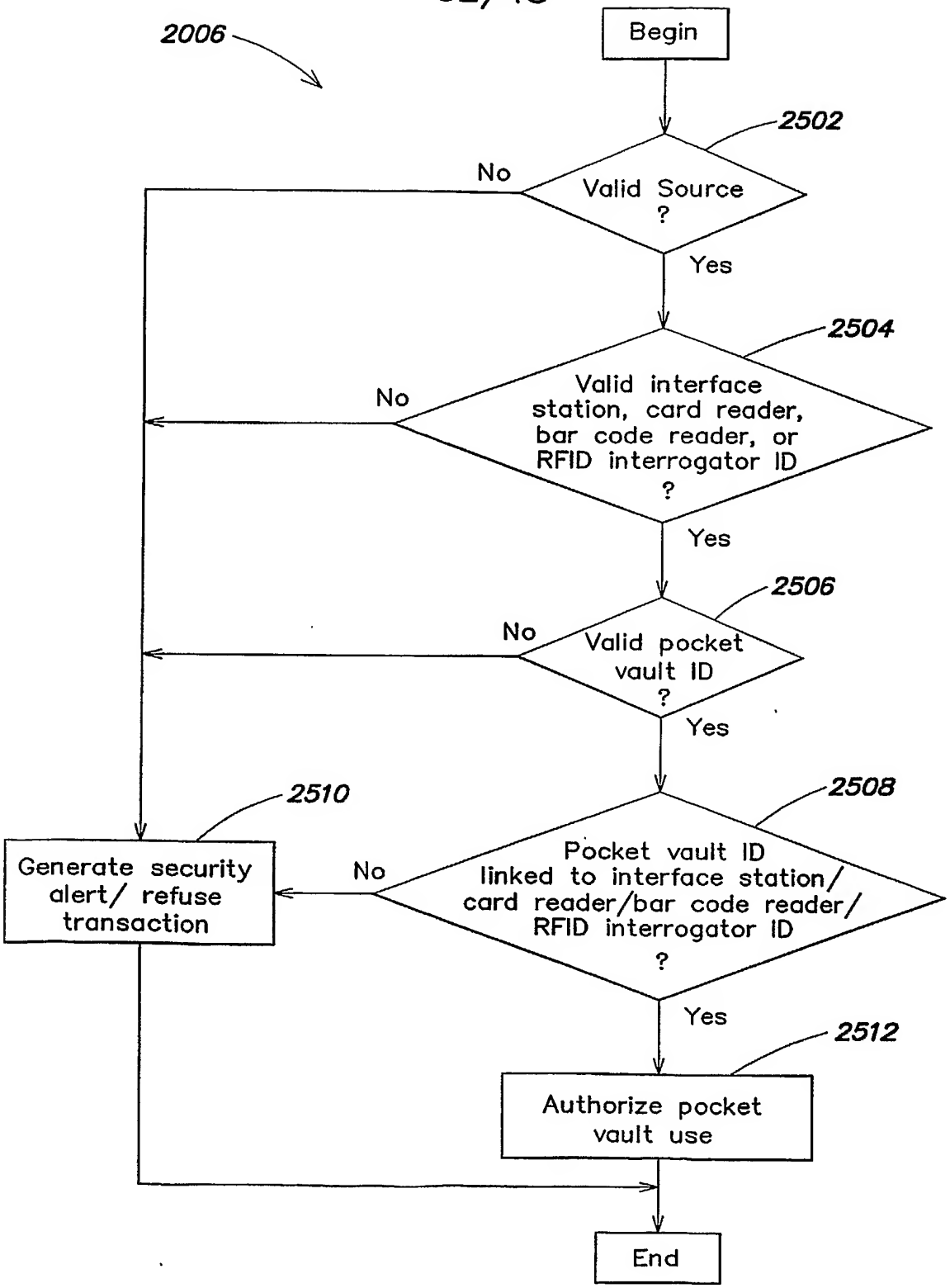

2006
Begin
2502
Valid Source ?
No
Yes
2504
Valid interface station, card reader, bar code reader, or RFID interrogator ID ?
No
Yes
2506
Valid pocket vault ID ?
No
Yes
2508
Pocket vault ID linked to interface station/ card reader/bar code reader/ RFID interrogator ID ?
No
Yes
2510
Generate security alert/ refuse transaction
2512
Authorize pocket vault use
End

FIG. 25

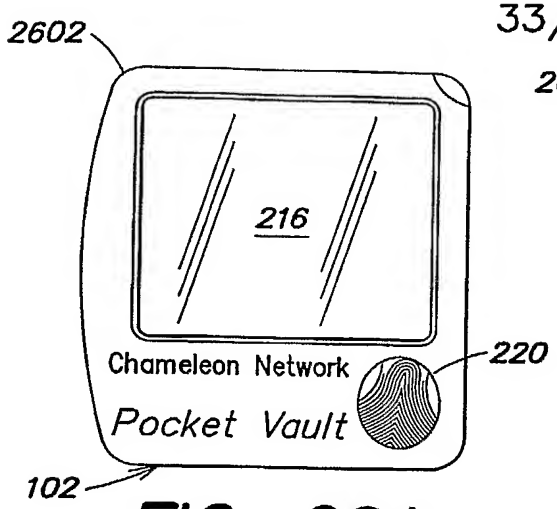


FIG. 26A

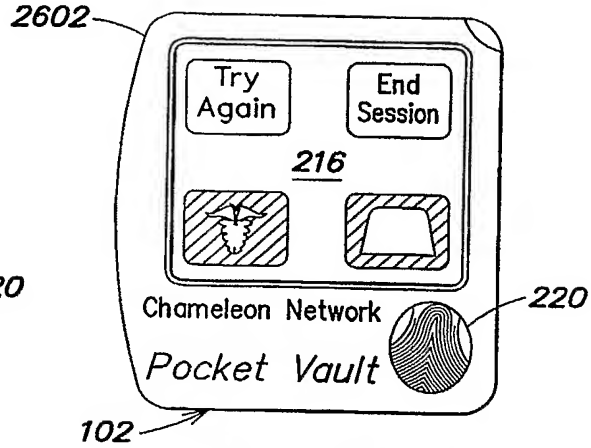


FIG. 26B

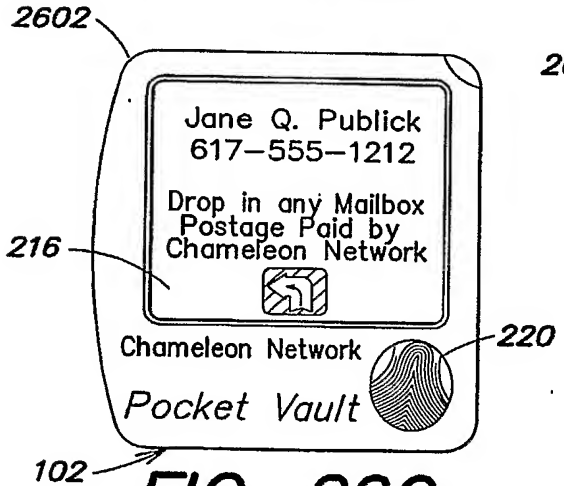


FIG. 26C

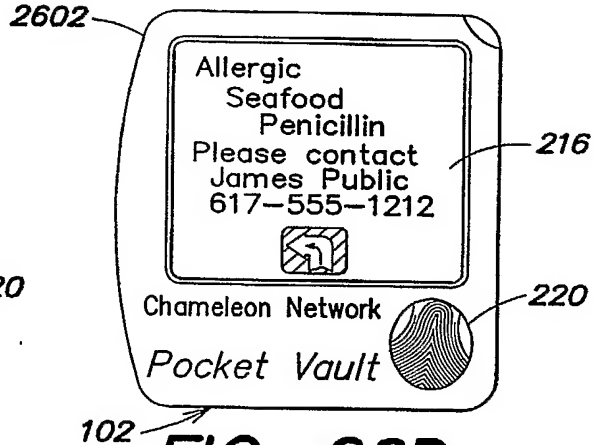


FIG. 26D

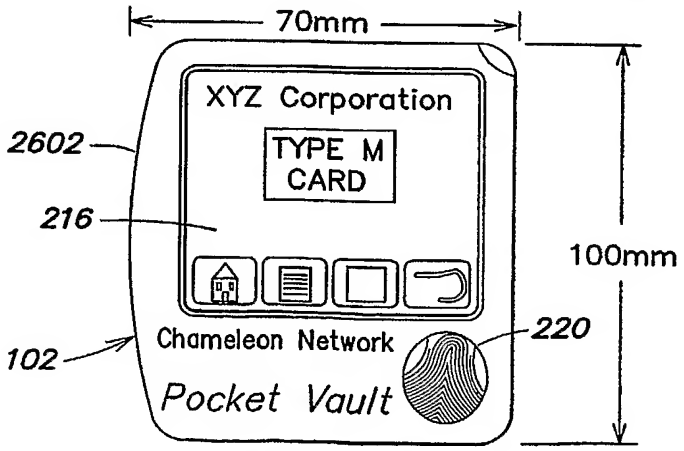


FIG. 26E

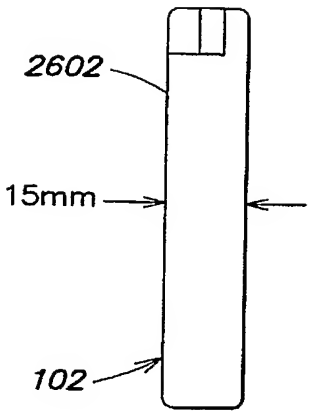


FIG. 26F

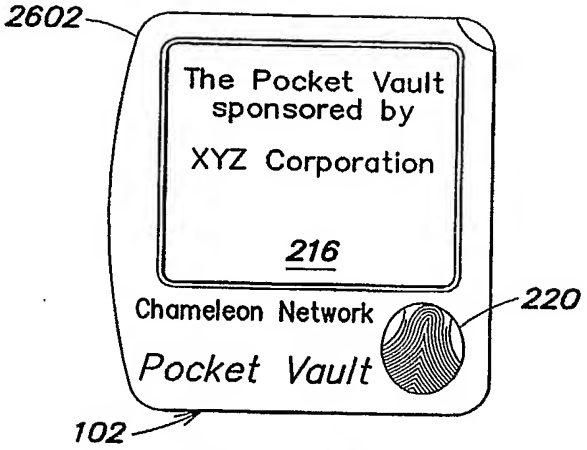


FIG. 26G

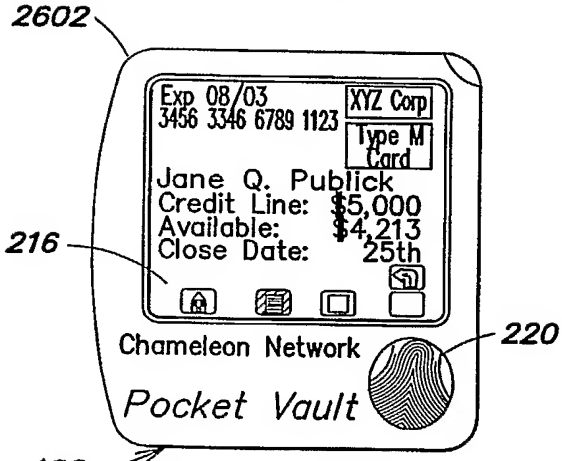


FIG. 26H

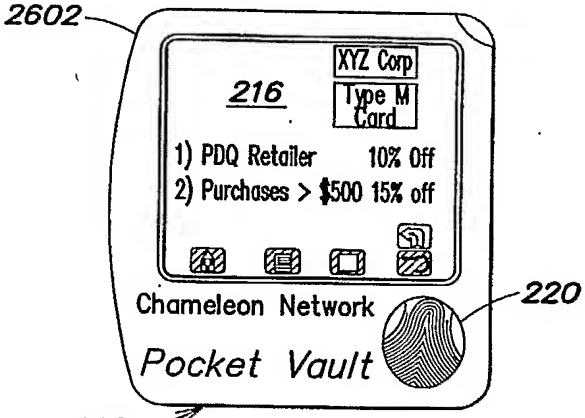


FIG. 26I

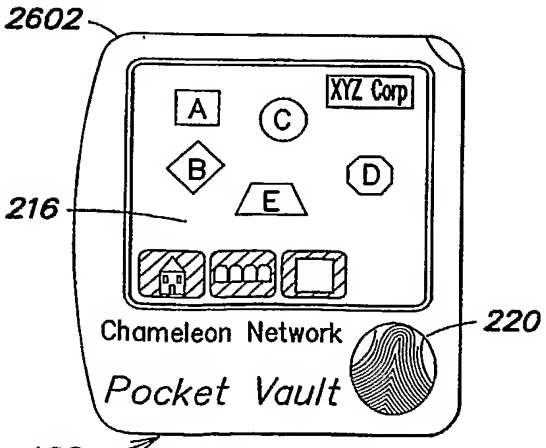


FIG. 26J

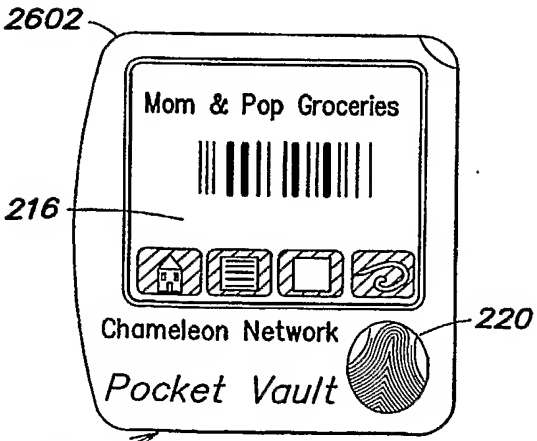


FIG. 26K

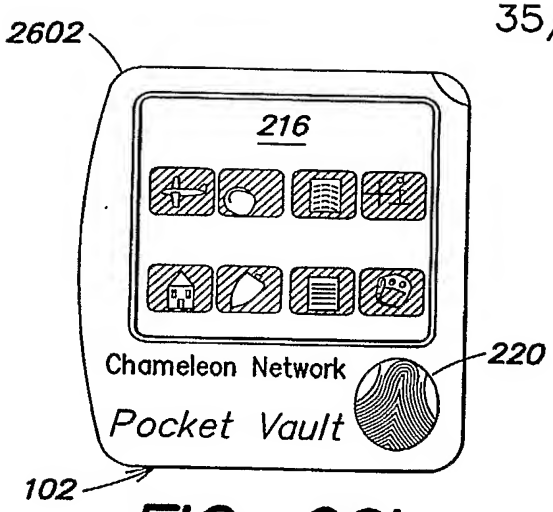


FIG. 26L

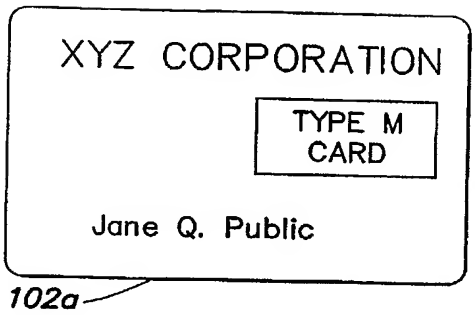


FIG. 26M

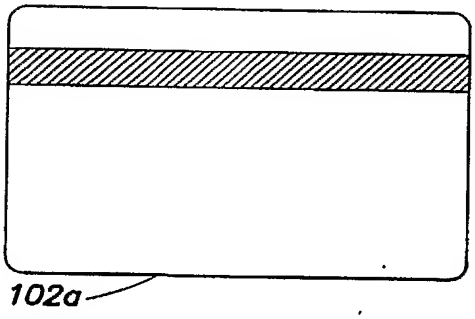


FIG. 26N

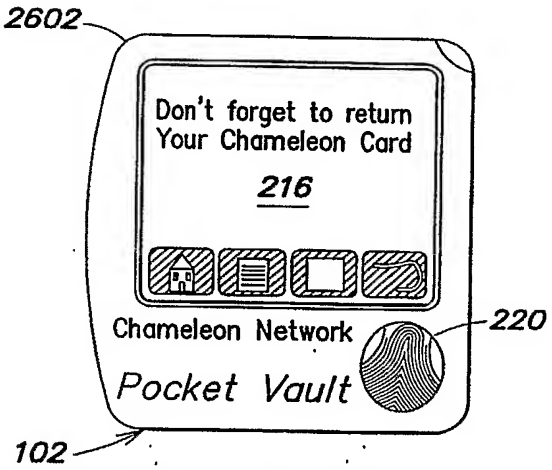


FIG. 260

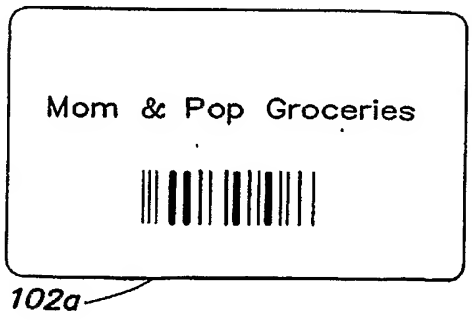


FIG. 26P

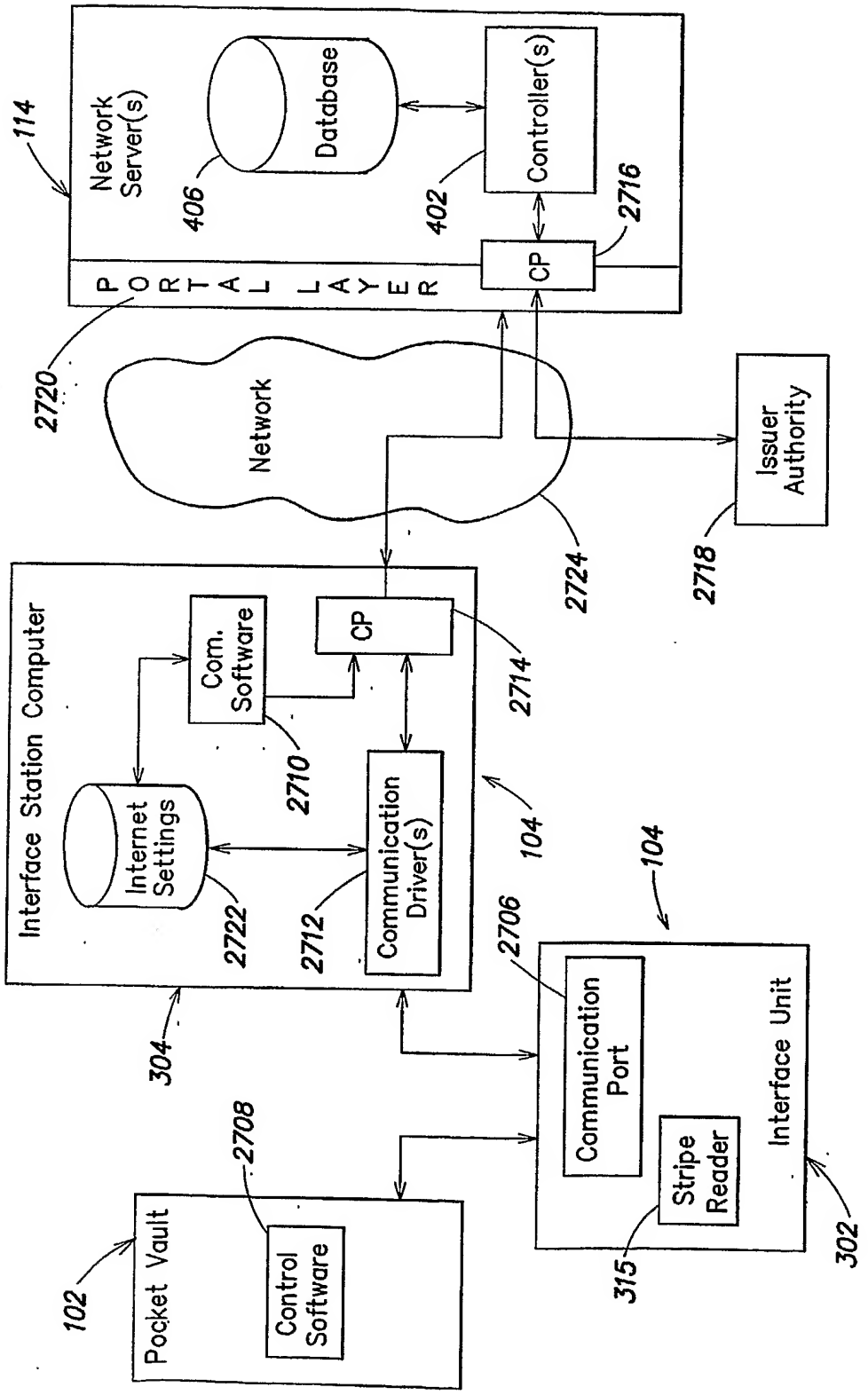

114
Network Server(s)
Database
406
Controller(s)
402
2716
PORTAL LAYER
CP
2720
Network
Issuer Authority
2724
2718
Interface Station Computer
Com. Software
CP
2714
2710
Internet Settings
2722
Communication Driver(s)
2712
104
104
2706
Communication Port
Stripe Reader
Interface Unit
315
302
304
2708
Control Software
Pocket Vault
102

FIG. 27

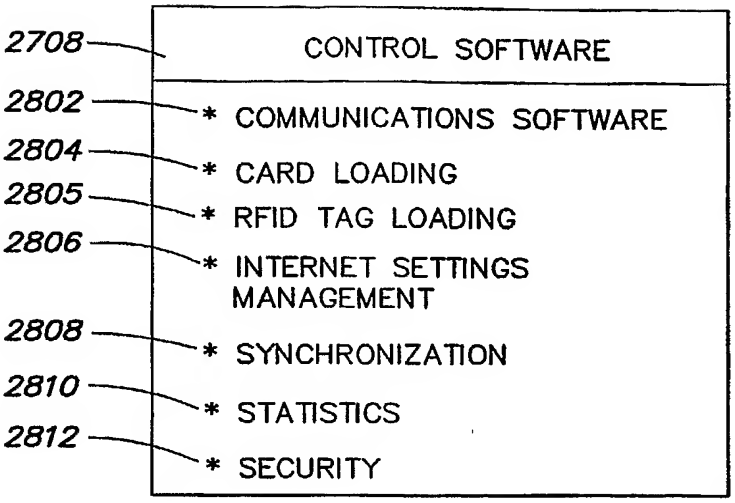

2708
CONTROL SOFTWARE
2802
* COMMUNICATIONS SOFTWARE
2804
* CARD LOADING
2805
* RFID TAG LOADING
2806
* INTERNET SETTINGS MANAGEMENT
2808
* SYNCHRONIZATION
2810
* STATISTICS
2812
* SECURITY

FIG. 28

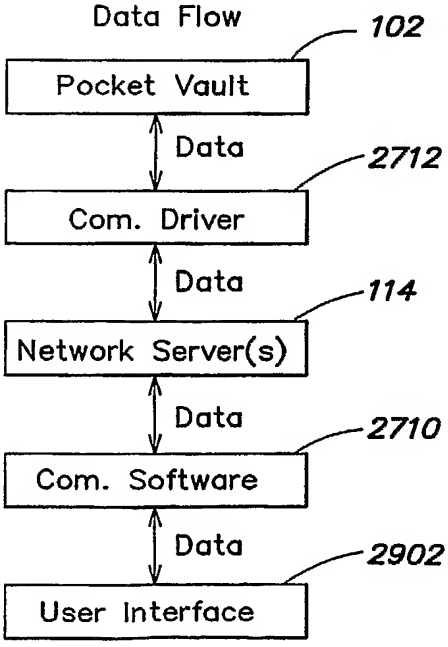

Data Flow
102
Pocket Vault
Data
2712
Com. Driver
Data
114
Network Server(s)
Data
2710
Com. Software
Data
2902
User Interface

FIG. 29

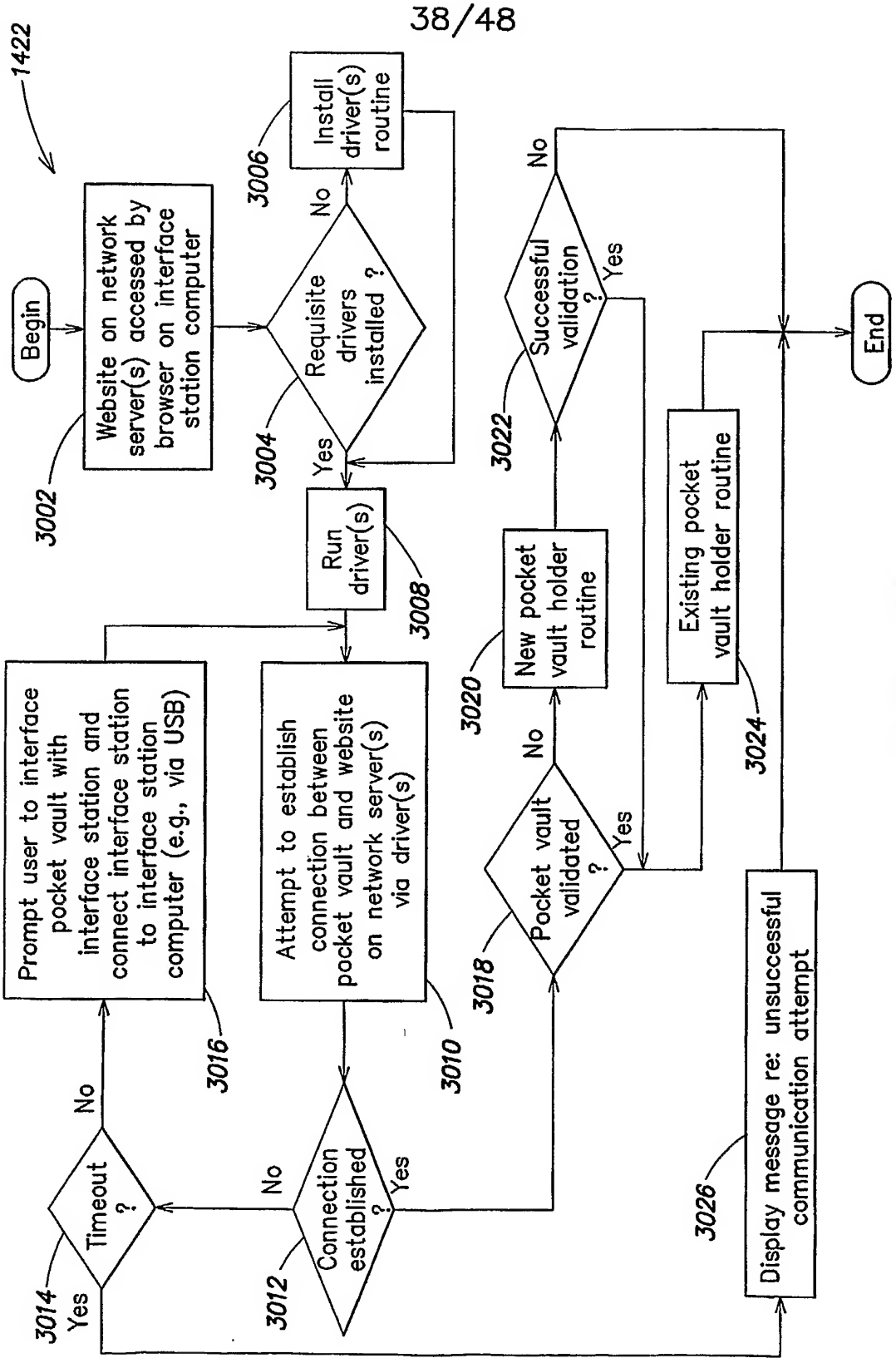

1422
Begin
Website on network server(s) accessed by browser on interface station computer
3002
Requisite drivers installed ?
3004
No
Yes
Install driver(s) routine
3006
Run driver(s)
3008
Prompt user to interface pocket vault with interface station and connect interface station to interface station computer (e.g., via USB)
3016
Attempt to establish connection between pocket vault and website on network server(s) via driver(s)
3010
Timeout ?
3014
Connection established ?
3012
Pocket vault validated ?
3018
New pocket vault holder routine
3020
Existing pocket vault holder routine
3024
Successful validation ?
3022
Display message re: unsuccessful communication attempt
3026
End

FIG. 30

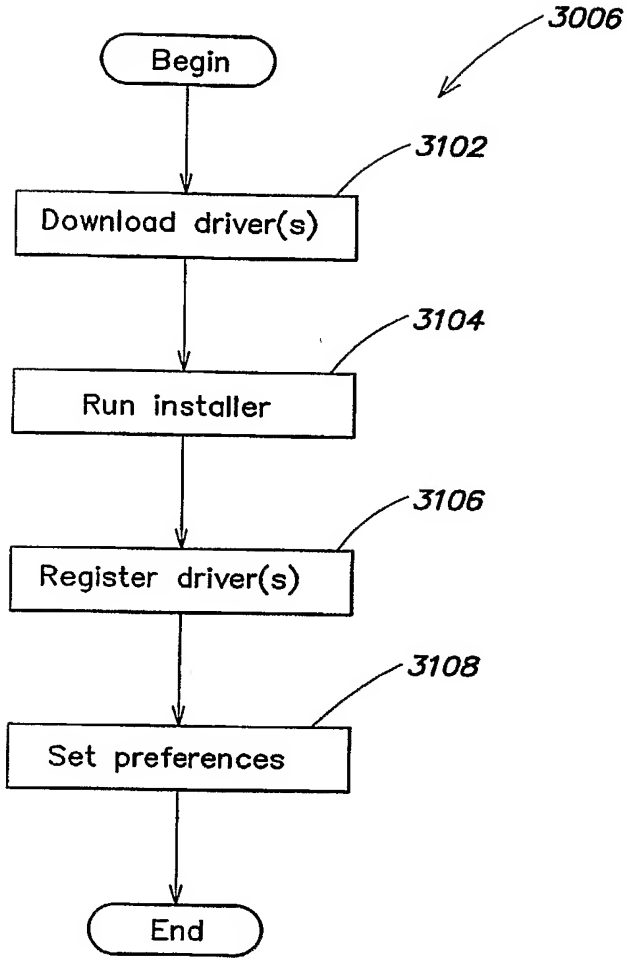

3006
Begin
3102
Download driver(s)
3104
Run installer
3106
Register driver(s)
3108
Set preferences
End

FIG. 31

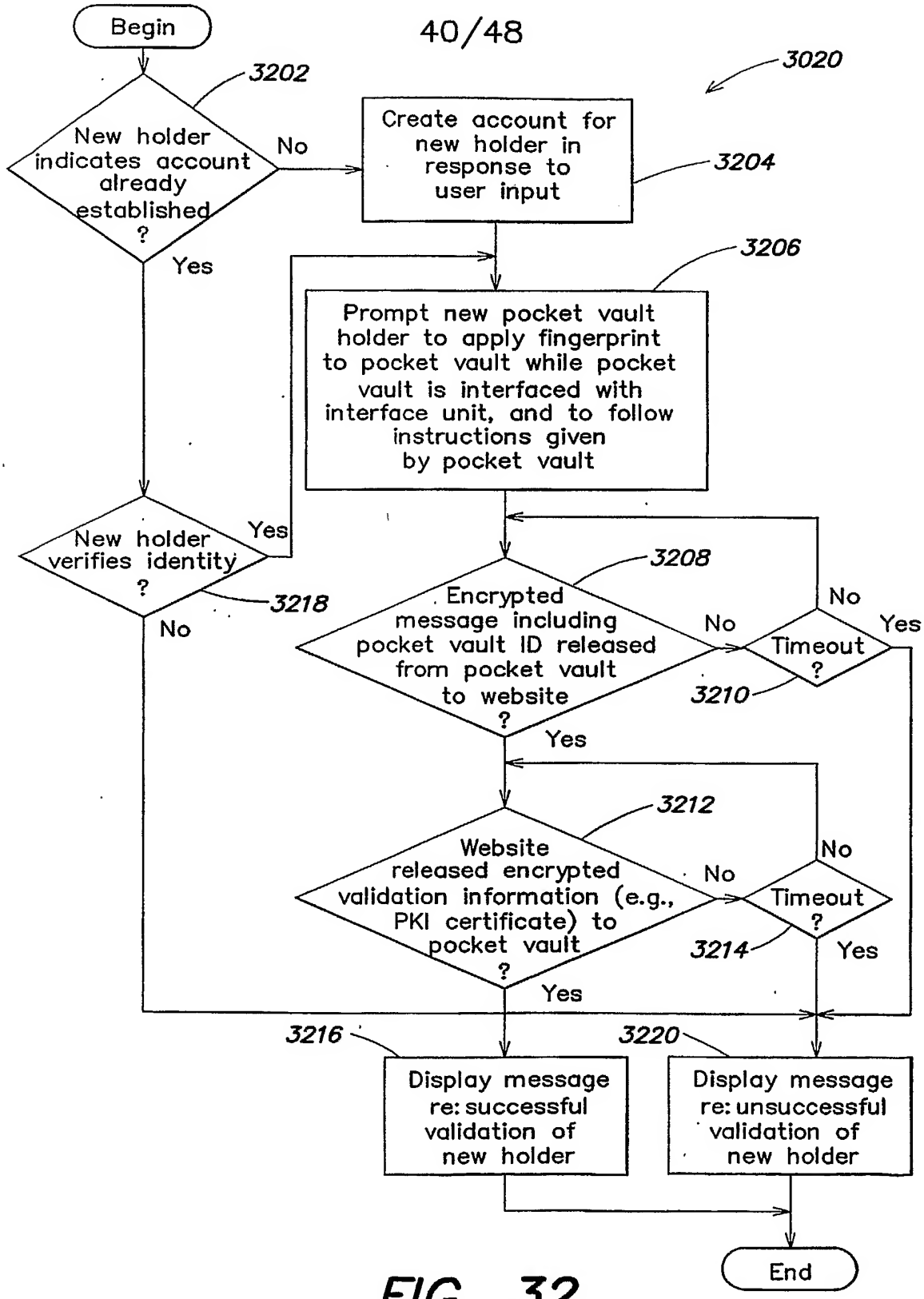

Begin
3202
New holder indicates account already established ?
No
Yes
3020
Create account for new holder in response to user input
3204
3206
Prompt new pocket vault holder to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit, and to follow instructions given by pocket vault
New holder verifies identity ?
Yes
No
3218
3208
Encrypted message including pocket vault ID released from pocket vault to website ?
No
Yes
Timeout ?
No
Yes
3210
3212
Website released encrypted validation information (e.g., PKI certificate) to pocket vault ?
No
Yes
Timeout ?
No
Yes
3214
3216
3220
Display message re: successful validation of new holder
Display message re: unsuccessful validation of new holder
End

FIG. 32

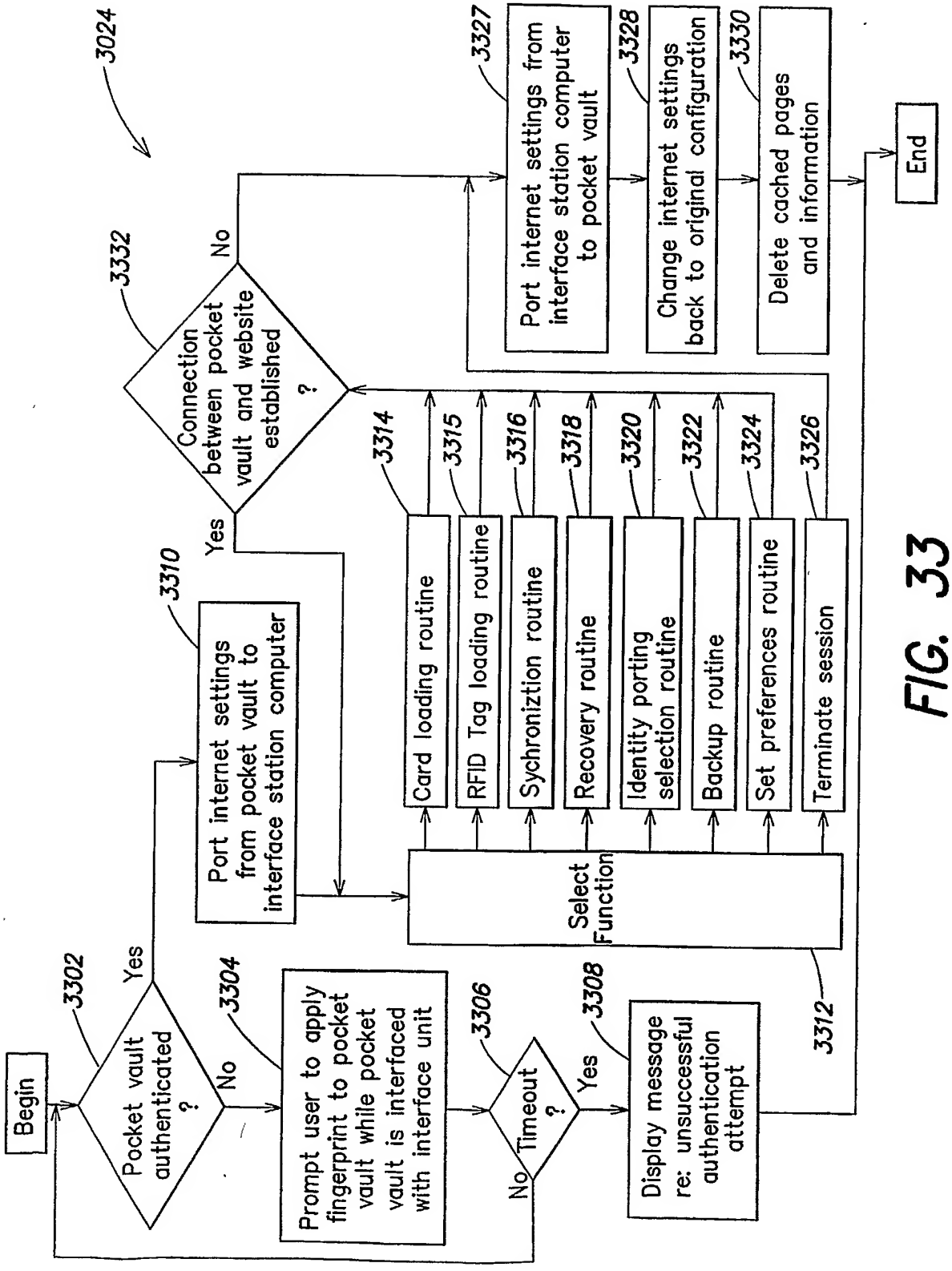

3024
Begin
3302
Pocket vault authenticated ?
Yes
No
3304
Prompt user to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit
3306
Timeout ?
No
Yes
3308
Display message re: unsuccessful authentication attempt
3310
Port internet settings from pocket vault to interface station computer
3312
Select Function
3314
Card loading routine
3315
RFID Tag loading routine
3316
Sychroniztion routine
3318
Recovery routine
3320
Identity porting selection routine
3322
Backup routine
3324
Set preferences routine
3326
Terminate session
3332
Connection between pocket vault and website established ?
Yes
No
3327
Port internet settings from interface station computer to pocket vault
3328
Change internet settings back to original configuration
3330
Delete cached pages and information
End

FIG. 33

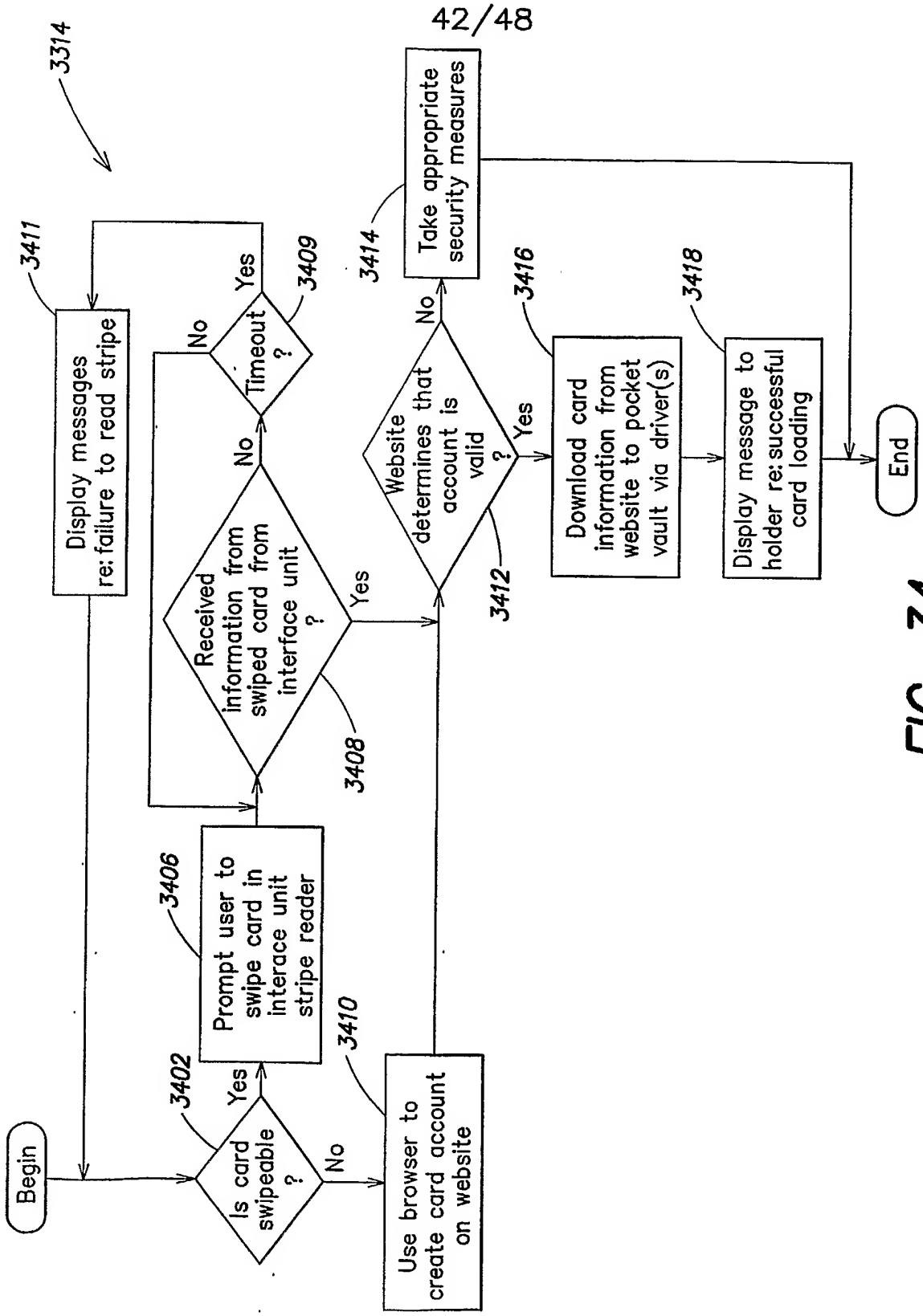

3314
Begin
Is card swipeable ?
3402
Yes
No
Prompt user to swipe card in interace unit stripe reader
3406
Use browser to create card account on website
3410
Received information from swiped card from interface unit ?
3408
No
Yes
Timeout ?
3409
No
Yes
Display messages re: failure to read stripe
3411
Website determines that account is valid ?
3412
No
Yes
Take appropriate security measures
3414
Download card information from website to pocket vault via driver(s)
3416
Display message to holder re: successful card loading
3418
End

FIG. 34

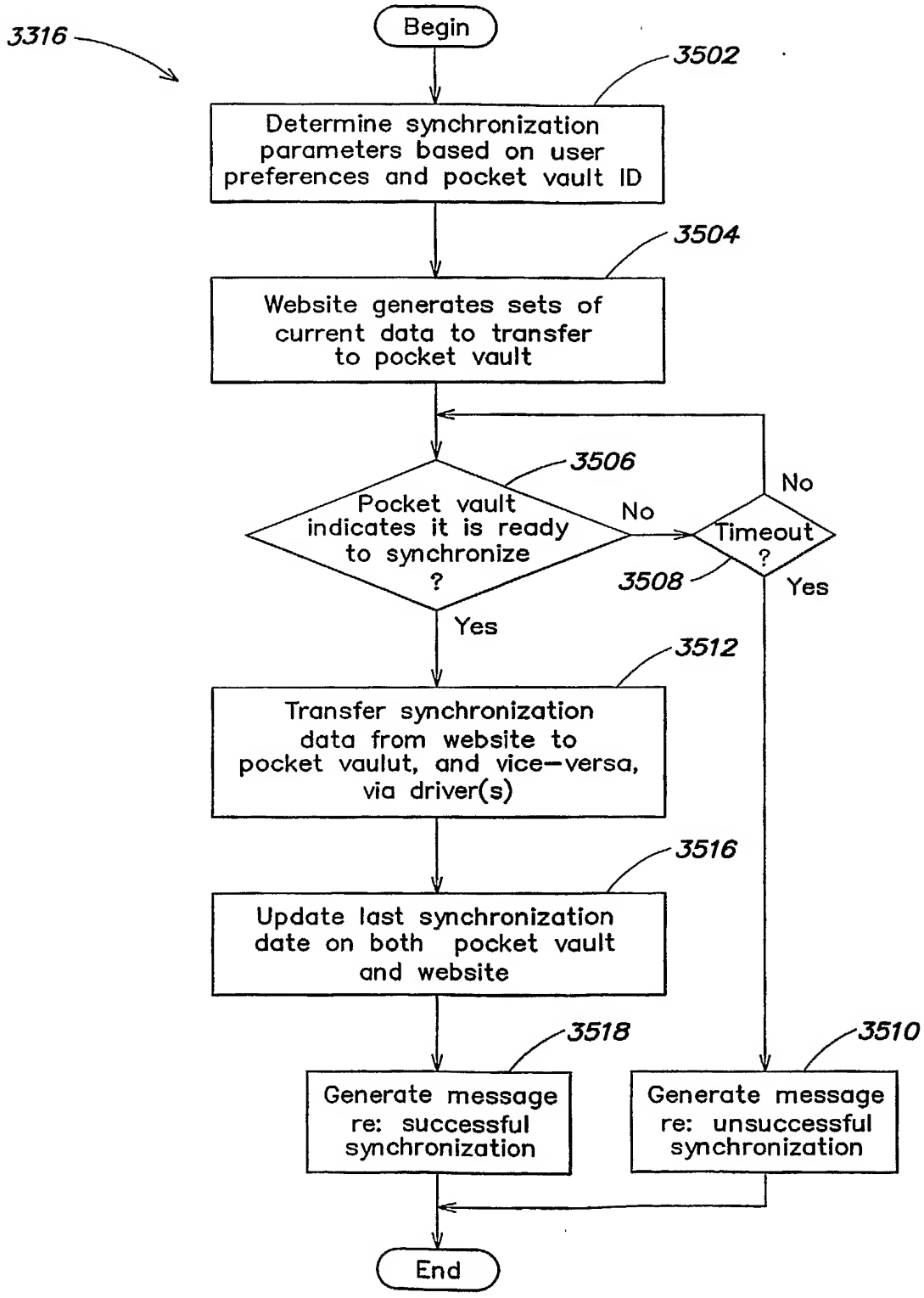

3316
Begin
3502
Determine synchronization parameters based on user preferences and pocket vault ID
3504
Website generates sets of current data to transfer to pocket vault
3506
Pocket vault indicates it is ready to synchronize ?
No
Timeout ?
No
Yes
3508
Yes
3512
Transfer synchronization data from website to pocket vaulut, and vice-versa, via driver(s)
3516
Update last synchronization date on both pocket vault and website
3518
Generate message re: successful synchronization
3510
Generate message re: unsuccessful synchronization
End

FIG. 35

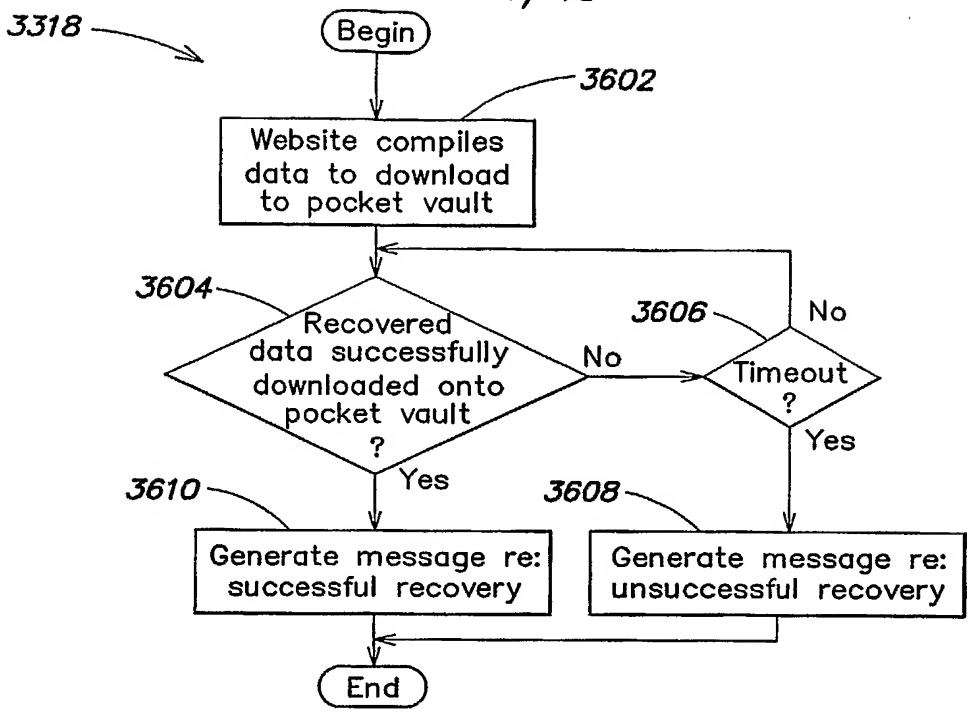

3318
Begin
3602
Website compiles data to download to pocket vault
3604
Recovered data successfully downloaded onto pocket vault ?
No
3606
Timeout ?
No
Yes
Yes
3610
Generate message re: successful recovery
3608
Generate message re: unsuccessful recovery
End

FIG. 36

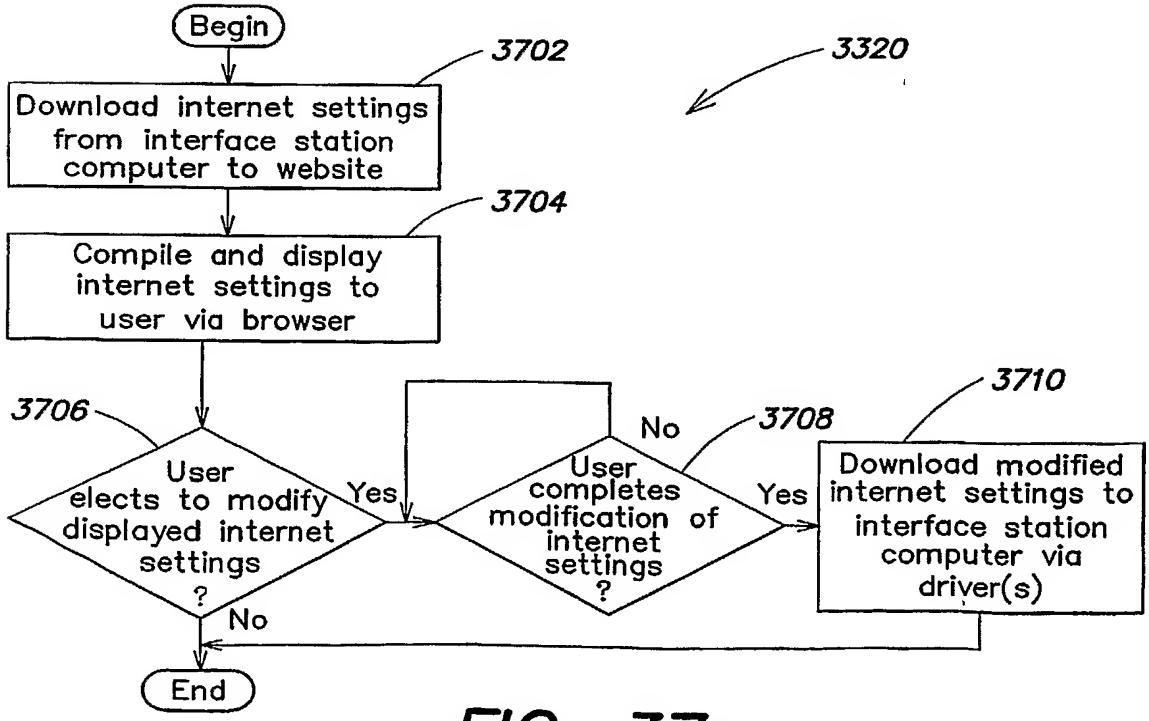

Begin
3702
Download internet settings from interface station computer to website
3320
3704
Compile and display internet settings to user via browser
3706
User elects to modify displayed internet settings ?
Yes
No
3708
User completes modification of internet settings ?
Yes
No
3710
Download modified internet settings to interface station computer via driver(s)
End

FIG. 37

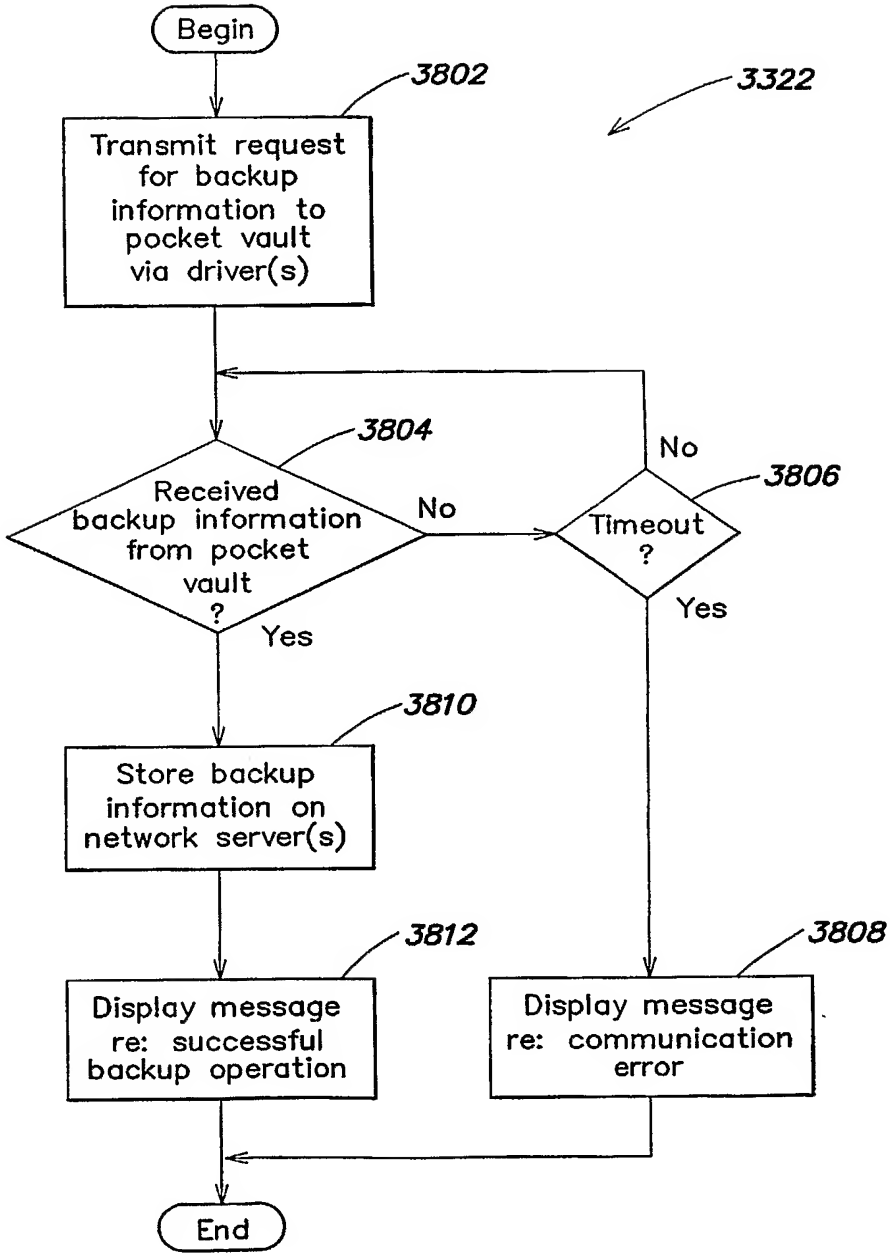

Begin
3802
3322
Transmit request for backup information to pocket vault via driver(s)
3804
Received backup information from pocket vault ?
No
Yes
3806
Timeout ?
No
Yes
3810
Store backup information on network server(s)
3812
Display message re: successful backup operation
3808
Display message re: communication error
End

FIG. 38

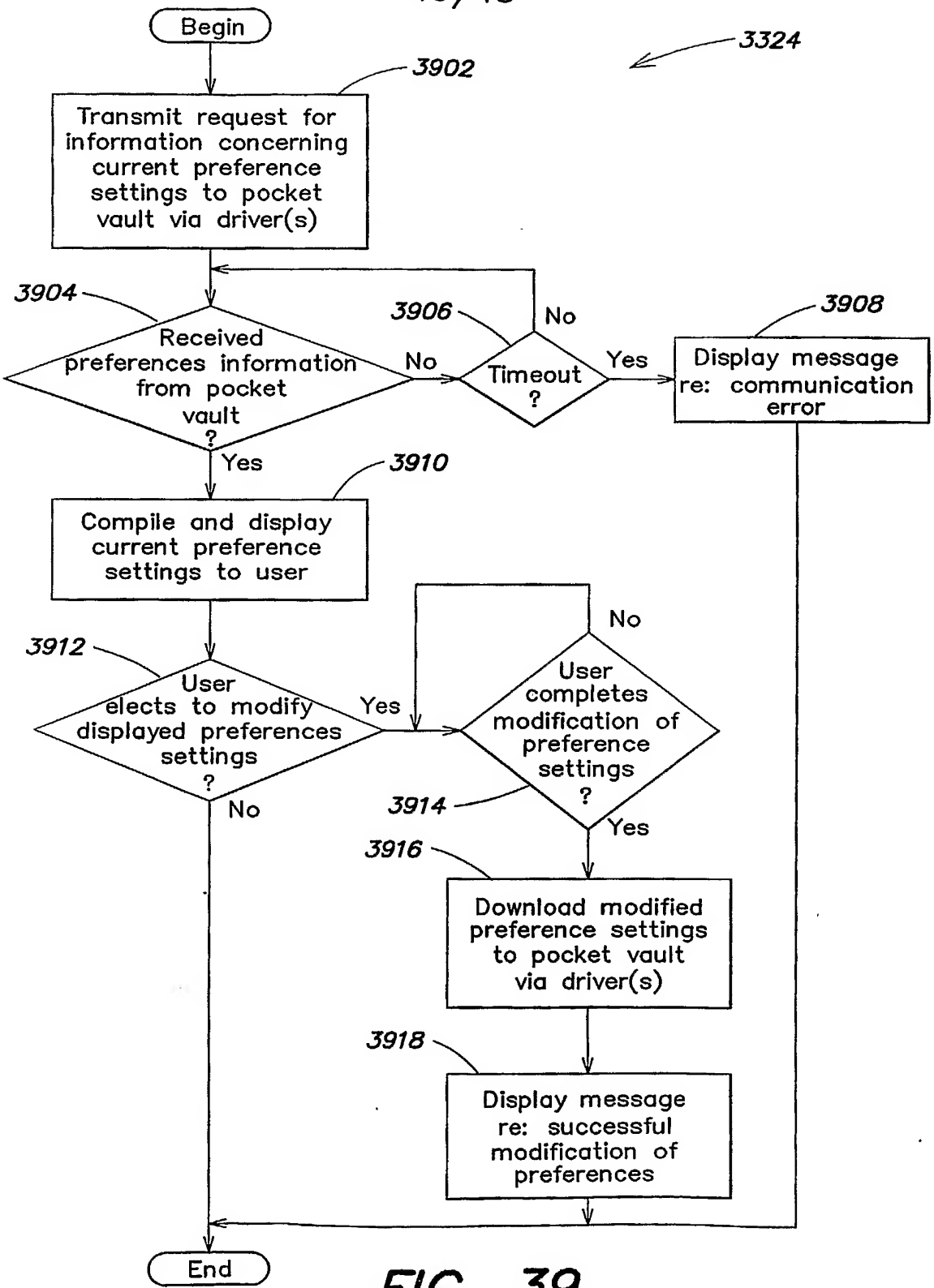

Begin
3324
3902
Transmit request for information concerning current preference settings to pocket vault via driver(s)
3904
Received preferences information from pocket vault ?
No
3906
Timeout ?
No
Yes
3908
Display message re: communication error
Yes
3910
Compile and display current preference settings to user
3912
User elects to modify displayed preferences settings ?
Yes
No
User completes modification of preference settings ?
No
3914
Yes
3916
Download modified preference settings to pocket vault via driver(s)
3918
Display message re: successful modification of preferences
End

FIG. 39

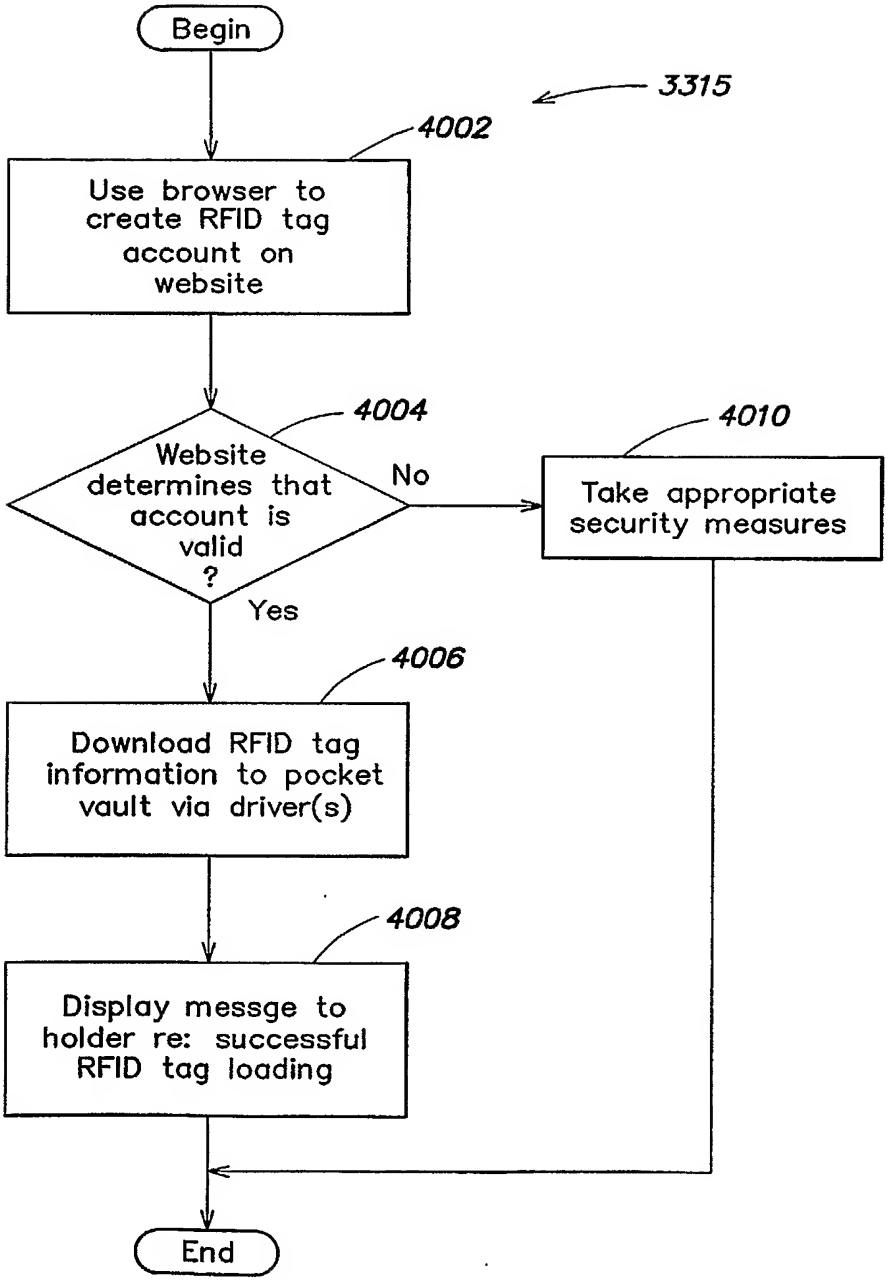

Begin
3315
4002
Use browser to create RFID tag account on website
4004
Website determines that account is valid ?
No
4010
Take appropriate security measures
Yes
4006
Download RFID tag information to pocket vault via driver(s)
4008
Display messge to holder re: successful RFID tag loading
End

FIG. 40

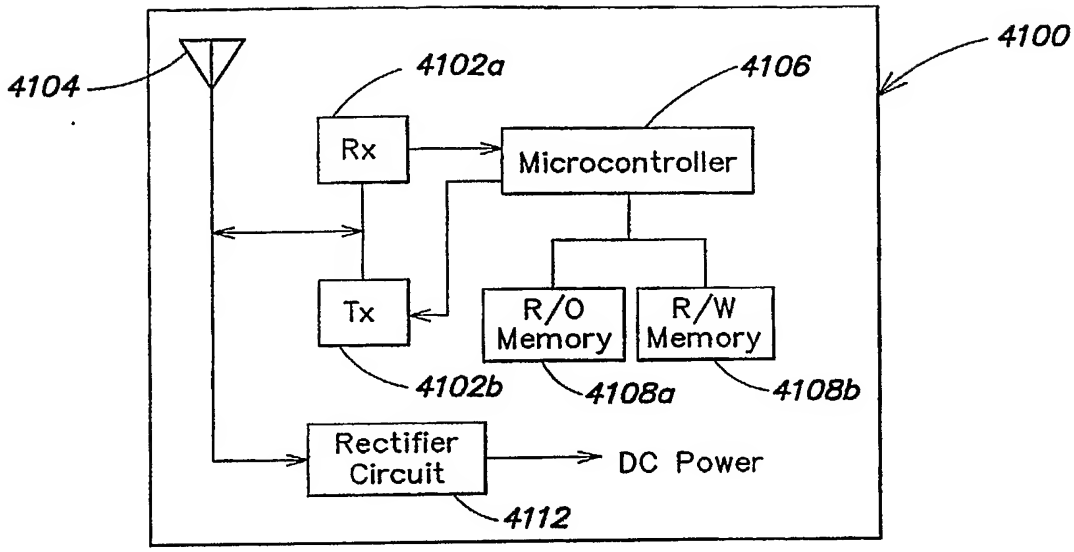


FIG. 41
(PRIOR ART)

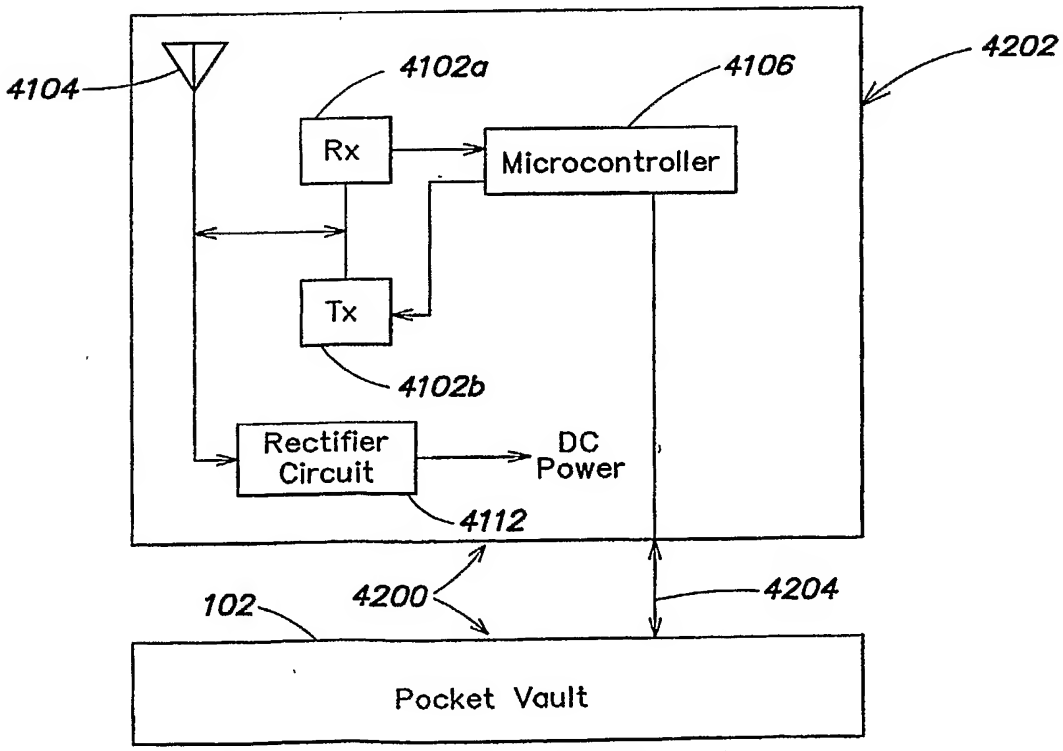


FIG. 42